RESISTING IMPERSONATION ATTACKS IN CHAINING-BASED PUBLIC-KEY MANAGEMENT ON MANETS
The Virtual Public-key Management

Renan Fischer e Silva, Eduardo da Silva and Luiz Carlos Pessoa Albini
NR2/LARSIS – Department of Informatics, Federal University of Paraná, Curitiba, Brazil

Keywords: MANET, Public-key management, Virtualization, Virtual structure.

Abstract: Chaining-based key management schemes seem to be the ones that best fit MANETs. The main chaining-based scheme is the Self-Organized Public Key Management System (PGP-Like). However, it is fully vulnerable to impersonation attacks. In order to reduce such vulnerability, this article introduces a new public-key management system for MANETs, the Virtual Key Management System (VKM). VKM uses a virtual structure to indicate the trust between nodes and the certificate chains formation. VKM can behave in a restrict way, being able to tolerate impersonation attacks to a certain level, or it can behave similarly to the PGP-Like, just by changing a simple parameter. Thus, VKM can suit any user needs switching between these two models dynamically, without any network reinitialization or reconfiguration.

1 INTRODUCTION

It is possible to classify the key management schemes for MANETs in (Djenouri et al., 2005): identity-based, chaining-based, cluster-based, predeployment-based and mobility-based. Among them, the chaining-based schemes appears to be the most suitable scheme to the MANETs environment. The main chaining-based key management scheme for MANETs is the *Self-Organized Public Key Management System* (Hubaux et al., 2001; Čapkun et al., 2003), called *PGP-Like* from now on.

PGP-Like is a self-organized public-key management scheme based on the PGP concepts, in which all pair-wised keys are created by the nodes themselves. Nodes also issue certificates to the other ones in which they trust. Each node has a local certificate repository that is periodically exchanged with its neighbors. Keys are authenticated through certificate chains which are built using the local certificate repositories.

As presented in (Silva et al., 2008), PGP-Like is highly vulnerable to the impersonation attack. Impersonation attacks consist on an attacker using false identities to deceive network protocols. The functionality of PGP-Like is compromised even with only 5% of Misbehaviour nodes in the network. In order to reduce such vulnerability, this article introduces a new chaining-based public-key management system for MANETs, the *Virtual Key Management System* (*VKM*). VKM uses a virtual structure to indicate the trust between nodes and the certificate chains formation. Virtual structures have already been used in routing protocols such as VRP (Albini et al., 2006) and VDV (Robba and Maestrini, 2007).

VKM is a flexible key management scheme. It can behave in a very restrict way, being able to tolerate impersonation attacks to a certain level, or it can behave similarly to the PGP-Like, just by changing a simple parameter. When VKM is set to a restrictive behavior, it is still able to correctly complete almost 80% of all key authentication requests with 5% of compromised nodes. Thus, VKM can suit any user needs with its ability to switch between the two models dynamically, without any network reinitialization or reconfiguration.

The rest of this paper is organized as follows: section 2 briefly describes the PGP-Like characteristics; section 3 details the Virtual Key Management Scheme; section 4 presents the Evaluation of the VKM, and a comparison with the PGP-Like; finally, section 5 draws the conclusions and future work.

Fischer e Silva R., da Silva E. and Carlos Pessoa Albini L. (2009).
RESISTING IMPERSONATION ATTACKS IN CHAINING-BASED PUBLIC-KEY MANAGEMENT ON MANETS - The Virtual Public-Key Management.
In *Proceedings of the International Conference on Security and Cryptography*, pages 155-158
DOI: 10.5220/0002236501550158

2 SELF-ORGANIZED PUBLIC KEY MANAGEMENT SYSTEM

The Self-Organized Public Key Management System, called PGP-Like, is a public key management scheme which uses certificate chains (Čapkun et al., 2003; Hubaux et al., 2001). Private and public keys of nodes are created by the nodes themselves following the PGP concepts (Zimmermann, 1995). In addition, each node issues public key certificates to other nodes in which it trusts. In PGP-Like, if a node u believes that a public key K_v belongs to node v, it issues a certificate binding K_v to the node v, $(v,K_v)_{prK_u}$, in which prK_u is the private key of node u. This certificate is stored in both nodes local certificate repositories. Furthermore, each node periodically exchanges its own repository with its neighbors.

Public keys and certificates are represented by a directed graph $G(V,A)$, in which V represents the public keys and A represents the certificates. A directed edge between two vertexes K_u and K_v, $(K_u \rightarrow K_v)$, denotes a certificate, signed by node u, binding K_v to node v. Each node u maintains an updated local certificate repository, G_u, and a non-updated local certificate repository, G_u^N, which contains the certificates that have expired.

When node u wants to authenticate the public key K_v of node v, it must find a path connecting K_u and K_v, represented by $(K_u \rightsquigarrow K_v)$. It firstly tries to find $(K_u \rightsquigarrow K_v) \in G_u$. If $\neg\exists(K_u \rightsquigarrow K_v) \in G_u$, node u merges G_u with G_v, $G' = G_u \cup G_v$, and it tries to find $(K_u \rightsquigarrow K_v) \in G'$. If a path exists, the authentication succeeds.

The use of certificate chains makes PGP-Like highly vulnerable to impersonation attacks, as shown in (Silva et al., 2008). An attacker, node x, can create a false identity m and issues a certificate binding k_m to m. Thus, if node x maintains a correct behavior during a considerable time, several units will, probably, trust it and the false identity will be spread over the network due to the certificate exchange mechanism.

3 VIRTUAL KEY MANAGEMENT SYSTEM

The Virtual Key Management System (VKM) uses a *virtual structure* to indicate the trust between nodes and the certificate chains formation. The virtual structure is represented by a directed graph $L(N,E)$, which is unrelated to the actual network topology. Set N represents the nodes and set E represents the virtual links. A virtual link $(i,j) \in E$ indicates that node i issues a certificate binding K_j to node j. Note that node i must do this for each node to which it has a direct connection in the virtual structure. For example, the virtual structure can be a RoR, a hypercube, a CCC or a torus, though results reported in this paper were obtained using the *Rings of Rings* (RoR) structure.

The *Rings of Rings* (RoR) structure is based on the following: assume that there are two integers, x and y, such that, $x * y = n$, and let s be an integer such that $1 < s \leq y$. Set N is partitioned into x rings, called $N_0, N_1, ..., N_{x-1}$, in which, for each $a \in [0,x)$, $N_a = \{i : a*y \leq i < (a+1)*y\}$. Link (i,j) belongs to E iff either $j \; mod \; y = (i+d) \; mod \; y$ for some $1 \leq d < s$ or $j = (i+y) \; mod \; n$. A notable feature of RoR structure is the redundancy of virtual paths, whose degree is determined by parameters x, y, and s. In VKM s is the number of certificates that a node issues. Figure 1 exemplifies the Ring of Rings (RoR) structure.

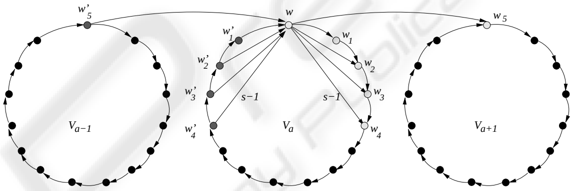

Figure 1: RoR Virtual Structure.

In VKM each node i creates its own pair of public and private keys, K_i and prK_i. Afterwards, it must issue certificates following the virtual structure. A pair of nodes in the virtual structure must exchange its keys through a secure channel. When a certificate is issued, its issuer stores it in a local repository and sends it to the correspondent node. All certificates are issued with a limited lifetime T_v.

VKM can behave in a restrict way, being able to tolerate impersonation attacks to a certain level, or it can behave similarly to the PGP-Like, just by changing a simple parameter. The main difference between these behaviors is the way nodes authenticate public-keys. Both forms will be presented next.

In VKM with reactive authentication (VKM-RA), each node maintains only its initial certificates, the certificates issued by it and the ones issued to it, thus reducing the memory needed by the local certificate repositories. When node i wants to authenticate the public-key of node j, it must find a virtual path from i to j, a certificate chain, in the virtual structure. After choosing a virtual path, thesource must gather all certificates to validate the entire virtual path as follows: (*i*) the first certificate is directly verified by node i using its own public key, as it is the issuer; (*ii*) each remaining certificate can be verified using the public key contained in the previous certificate; (*iii*) the last certificate contains the public key of node j.

VKM with proactive authentication (VKM-PA) behaves similarly to PGP-Like. Though certificates are issued following the virtual structure, nodes periodically exchanges their certificate repositories with their physical neighbors. . When a node i wants to authenticate the public key K_j of node j, it tries to find a certificate chain in its local repository, $(K_i \rightsquigarrow K_j) \in G_i$. If $\exists(K_i \rightsquigarrow K_j) \in G_i$, it performs the authentication using VKM-PA. If $\neg\exists(K_i \rightsquigarrow K_j) \in G_i$, node i, node i invokes VKM-RA. This characteristic makes the authentication more effective than PGP-Like, as it is possible to reach all nodes using the VKM-RA.

4 EVALUATION

The Network Simulator 2 (NS-2) (NS-2, 2007), version 30, was used to evaluate VKM. The parameters used in the simulations are presented in table 1. All simulations results are averages of 35 simulations with 95% of confidence interval.

Table 1: Simulation scenarios.

Parameter	Value
Network dimension	1000 x 1000 meters
Transmission range	120 meters
Nodes	100
Mobility model	random waypoint
Max. speed	20 m/s
Max. pause time	20 seconds
Exchange certificate interval	60 seconds
Simulation time	1500 seconds
Propagation Model	two-ray ground
MAC	802.11
RoR	x=4, y=25, s=5

VKM was evaluated under two different network behaviors: (*i*) under the impersonation attack and (*ii*) under the lack of cooperation attack. The evaluation under the impersonation attack demonstrates that VKM-RA can tolerate several misbehavior nodes in the network, while PGP-Like is completely vulnerable even with only 5% of misbehavior nodes (Silva et al., 2008). The evaluation under the lack of cooperation attack was made to demonstrate that the behavior of VKM-PA is similar to PGP-Like. The results shown here for PGP-Like are from (Silva et al., 2008).

4.1 Impersonation Attack

As VKM-RA must use the virtual structure in all authentications, a valid impersonation attack must be an impersonation of a node within the virtual structure. Otherwise, the attack is useless, as no authentication would use such a node.

Simulations scenarios consider 5%, 10%, 20% and 40% of misbehaviour nodes. They also consider $s = 5$, $s = 10$, $s = 15$ and $s = 20$ certificates issued to and by each node. As shown in figure 2, even with 20% of misbehaviour nodes in the network, VKM-RA is still able to authenticate several certificate chains. In the presence of 5% of misbehaviour nodes, VKM-RA is able to correctly authenticate almost 80% of the certificate chains, while PGP-Like is completely compromised even with only 5% of attackers (Silva et al., 2008).

VKM-RA can tolerate impersonation attacks better than PGP-Like due to the virtual structure, as the virtual structure is highly redundant and it establishes several “fixed” chains for authentication. If the number of compromised nodes is small, it is possible to avoid compromised nodes simply by randomly choosing the certificate chain. It is also possible to implement a misbehavior detection mechanism, thus nodes might explicitly avoid compromised nodes.

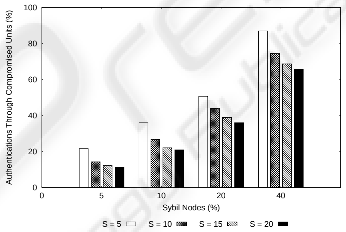

Figure 2: Authentications Through Compromised Nodes.

Figure 2 also shows that with 40% of misbehaviour nodes and 5 issued certificates, the possibility of choosing a compromised chain reaches more than 80%. However, this percentage is reduced to almost 60% if the number of issued certificates is increased to 20, thus demonstrating that increasing the node connectivity in the virtual structure, it is possible to reduce the effects of the impersonation attack. However, it is still possible to have efficient attacks on VKM-RA: attackers could organize a cooperative attack to a node of the virtual structure and separate it from the rest of the network.

4.2 Lack of Cooperation Attacks

To demonstrate that VKM-PA behaves similarly to PGP-Like, VKM-PA was evaluated under the Lack of Cooperation Attack and its results are compared with the ones provided by (Silva et al., 2008). These simulations consider 5%, 20%, 40% and 60% of selfish nodes. Following the results presented in (Čapkun et al., 2003) and (Silva et al., 2008) to evaluate the PGP-Like, two metrics are used in this evaluation: *CE* (Certificate Exchange Convergence) and *UR* (User Reachability).

Figures 3 and 4 illustrate the VKM-PA behavior under lack of cooperation attacks. In both, VKM-

PA results are compared with PGP-Like ones. As expected, increasing the number of attackers, CE value decreases (Figure 3). In scenarios without attackers or with 5% up to 60% of attackers, VKM-PA presents the same behavior of PGP-Like. *UR* results for VKM-PA with up to 60% of selfish nodes are also similar to those of PGP-Like (Figure 4). *UR* is almost 100% even in the presence of 60% of selfish nodes, the same behavior found on PGP-Like.

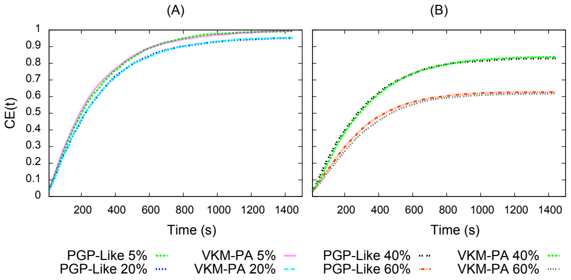

Figure 3: Convergence of Certificate Exchanges.

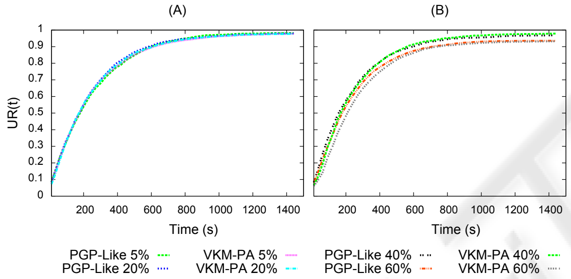

Figure 4: User Reachability.

5 CONCLUSIONS AND FUTURE WORK

Chaining-based key management schemes seem to be the ones that best fit the MANET paradigms. The main chaining-based scheme is the Self-Organized Public Key Management System (PGP-Like). However, as presented in (Silva et al., 2008), PGP-Like is highly vulnerable to the impersonation attack. The functionality of PGP-Like is compromised even with only 5% of misbehaviour nodes in the network.

This article introduces a new chaining-based public-key management system for MANETs, the Virtual Key Management System (VKM). VKM is a flexible key management scheme. It can be configured to work in two different ways, VKM-RA and VKM-PA. VKM-RA has a restrictive behavior. Using VKM-RA, nodes follow the rules of the virtual structure to issue certificates and authenticate keys. As showed in simulations, only few misbehaviour nodes in a disorganized way cannot effectively compromise the network behavior. VKM-RA is still able to correctly complete almost 80% of all key authentication requests with 5% of compromised nodes. Furthermore, VKM can behave similarly to PGP-Like just by changing a simple parameter, VKM-PA.

Future work includes the test of VKM under different kinds of attacks. It also includes the development of a secure version of the VRP routing protocol using VKM as the key management scheme.

REFERENCES

Albini, L., Caruso, A., Chessa, S., and Maestrini, P. (2006). Reliable routing in wireless ad hoc networks: The virtual routing protocol. *Journal of Network and Systems Management*, 14(3):335–358.

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.

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.

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

NS-2 (2007). The network simulator - ns-2.

Robba, A. and Maestrini, P. (2007). Routing in mobile ad-hoc networks: The virtual distance vector protocol. In *Proceedings of the IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS 2007)*, pages 1–9.

Silva, E., dos Santos, A. L., Albini, L. C. P., and Lima, M. N. (2008). Quantify misbehavior attacks against the self-organized public key management on manets. In *Proceedings of the International Conference on Security and Cryptography (SECRYPT 2008)*, pages 128–135.

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