PERFORMANCE OF VOUCHER SYSTEM FOR IMPLANTED CHAIN CERTIFICATE SCHEME

Ladislav HURAJ
Department of Computer Science, Faculty of Natural Sciences, Matthias Bel University,
Tajovského 40, 974 01 Banská Bystrica, Slovakia, tel. 048/413 9823, e-mail: huraj@fpv.umb.sk

SUMMARY

The paper presents design, background as well as simulation results of our new communication system designed for ad-hoc wireless networks which supports Implanted Chain Certificates Scheme providing efficiency of certificate verification. We employ threshold cryptography to spread the certificate service over specially selected nodes, the vouchers, to achieve high fault tolerance against network partition and malicious nodes. Moreover, we present ubiquitous services of Implanted Chain Certificates Scheme in the network by voucher system and we provide some insights into the configuration of such security services in ad-hoc networks. Simulations by use of ns2 simulator confirm the effectiveness of our design.

Keywords: *Ad-hoc networks, certificate chain, voucher, simulation.*

1. INDRODUCTION

A wireless ad-hoc network is a network where two or more devices communicate with each other using wireless transmission without the required intervention of any centralized access point or existing infrastructure. The topology in ad-hoc networks can change rapidly as nodes move in and out of each other's range. Since the topology of ad-hoc network changes dynamically, all mobile nodes act as routers and route packets for each other. There are special adaptive routing protocols applied like Dynamic Source Routing (DSR) [1], Ad Hoc On Demand Distance Vector Routing (AODV) [2] or Destination Sequenced Distance Vector Routing (DSDV) [3]. Ad-hoc networks are suitable for many applications, rescue, emergency and civil defense operations, team working applications, military actions, virtual classrooms or even local area networks.

Authorization certificates are used for efficiency of access control in ad-hoc networks. The authorization certificate possesses access permissions to an entity, which is trustworthy for the certificate issuer. Moreover, every other entity, which obtained a certificate from a trustworthy entity, can be trustworthy for the issuer as well. In this way a sequence of certificates, the chain of certificates is formed. Chains of certificates can improve the capability and manageability of the authorization process, the responsibility is distributed among several users and a user does not have to manage the authorization of each entity itself.

We consider the following scenario: a meteorological office (MeteO) which gathers weather, pollution, and other environmental data. MeteO consists of a center, but also of many particular static or mobile stations which can work independently of MeteO center, as well as of individual field scientists in distributed environmental sensors. All these parts of the meteorological office are called MeteO members.

MeteO members can communicate with each other, share their results and exchange their particular field measurements. Because members can change their position in a landscape area, they use an ad-hoc network for communication. The MeteO membership is delegated through chains of delegation certificates. Moreover, cooperative institutions or cooperative research partners can be allowed to utilize the measure results as well as exchange particular measurements with MeteO members during their mutual project. They obtain the rights either directly from the MeteO center or from a cooperation station, possibly from individual scientists which head the project, and they become MeteO members during the project. Cooperative partners can also delegate the membership to their partners for the period of the project, they can delegate them to their partners, etc. This possibility can cause an extreme increase of certificate chain length; e.g. with hundreds of certificates.

A member from MeteO group, wanting to obtain direct information for example from a sensor, has to prove his authority. For this, the member has to show its certificate chain to prove its membership; the chain must start with the MeteO center. Generally, the chains of certificates are used not only to confirm membership but also to document who authorized the membership. However, the size of certificate chains in such delegation system could be extremely high. One way for reducing of verification time of certificate chains are Implanted Chain Certificates [4].

This paper focus on simulations results of new ad-hoc networks system for scheme of Implanted Chain Certificates providing efficiency of certificate verification. In Section 2, we will describe the distributed group membership management, Implanted Chain Certificate as well as related works. Section 3 will outline the role of the issuer of this kind of certificate as well as the principle of whole voucher system. In Section 4 simulation results from our implementation of the proposed scheme will be presented. Finally, the Section 5 concludes this paper.

2. BACKGROUND

Our new ad-hoc networks system was proposed for Implanted Chain Certificates scheme built upon distributed group membership management. In the following, we give a brief overview of distributed group membership management and Implanted Chain Certificate as well as state of the art systems.

2.1. Distributed Group Membership Management for ad-hoc networks

This subsection is a short extract about the idea of distributed group membership management for ad-hoc networks from [5,6]. A group within group membership management is a set of members, persons or other physical or logical entities that may collectively be given access rights [5].

Membership management is based on public-key certificates; each member in the group possesses its own certificate proving its membership. The certificate is issued directly to the member public key. New group is established by special member – *group-key owner*. The group-key owner generates and possesses a new key pair – the group key, which identifying the group. The position of the group public key is special. Everyone dealing with the group will automatically know it. Each member of the group is identified by its respective public keys and obtains a certificate signed by the private group key to certify membership of the group. Verification of the certificate is performed with the public group key.

Moreover, the group-key owner can certify leaders who possess the same authority as the group-key owner, i.e. the leader can certify a new member into the group as well as to appoint other leaders and to issue membership certificate. A new leader obtains a leader certificate which was issued to its public key, the leader key. When a new member or leader is certified, it acquires its member/leader certificate as well as all certificates proving its status in the group starting with a certificate signed by the group-key owner. The certificates create a chain of delegation certificates and a member can prove its group membership by presenting its certificate chain [5].

The verification process of the chain consists of the verification of all certificates in the chain, of the checking of correct order of certificates, of checking of membership delegation authority as well as of time validation computation.

Adding, removing as well as authentication of users by certificate chains in Distributed Group Membership Management efficiencies the management of access rights in ad-hoc networks. On the other hand, the size of certificate chains could be too long to be practical [6]. Our solution how to reduce the verification time of the chains of certificates [4] through Implanted Chain Certificates is shortly described in next subsection.

2.2. Implanted Chain Certificate

Implanted Chain Certificate (IChC) is used to guarantee integrity and correctness of a chain of certificates [4]. IChC can be imagined as a certificate for a chain of certificates.

IChC guarantees:

(i) integrity of all delegation certificates in the certificate chain, i.e. the content of certificate has not been accidentally or maliciously modified

(ii) all signatures of all certificates in the certificate chain are legitimated

(iii) all certificates in the chain were signed in right order respectively starting with the private group key.

A chain of certificates must be verified before issuing of an IChC. In order to verify the certificate chain, the issuer of IChC needs the group public key. After the issuer checks the integrity and legitimacy of the chain and checks that the first certificate in a certificate chain is signed by the group key, it implants the whole chain as content of IChC and signs the IChC content with its digital signature. The issuer of IChC is called the *Voucher*.

The verification of IChC uses only a constant amount of cryptographic operations; therefore it is computationally more efficient when compared with the classical verification of the chain.

An IChC is issued to guarantee correctness of chain of certificates from a group-key owner to a certified member. Moreover, there is a special behaviour of IChC: if IChC certified the correctness of the whole certificate chain, it certified the correctness of any subchain of the chain as well. Consequently the IChC does not been issued to each member. When one member obtains its own IChC from the voucher, it can offer it to his previous leader in the chain, this leader to a previous leader, etc. The behaviour reduces the amount of issued IChCs.

More about IChC can be found in [4].

For realization of the IChC service in distributed group membership management it is necessary to possess for each voucher only simple certificate. Moreover, it is required that it works under ad-hoc network, i.e. it is not possible used central or hierarchical structure like in common certification systems.

2.3. State of the Art

Various systems use a concept of threshold secret sharing and secret share updates for certificate services in ad-hoc networks. The concept of threshold secret sharing is to distribute secret information among n members through their secret shares. No single entity in the network knows or holds the complete system secret. The aim is to allow any subset of k members to reconstruct the complete secret. This recovery of the secret is impossible for less than k members. Moreover, a

new member can obtain its new secret share which is computed directly from *k* secret shares.

Yi and Kravets [7] use threshold cryptography for certification services, where a node has to connect at least *k* of certification authorities for obtaining its certificate. Increasing of security is based on selected secure nodes called MOCAs (MObile Certificate Authority)s, that share the responsibility of collectively providing the CA functionality. For optimalization of the system direct-cast based on cache information instead of broadcasting is used. However if very fast change of network topology is occurred, the optimalization is ineffective.

Pathak and Iftode proposed in [8] a voting based protocol for authentification and for the group membership control. The trust decision in the system is based on collective voting of a group of *k* members. Malicious participants can be tagged as dishonest and expelled from trusted groups. This solution provides a good level of fault tolerance. Compared to certificates authorities based on threshold cryptography the system does not need distributor of secret shares and so does not concentrate failure into concrete nodes. Since the group does not posses only one key for signing, each member has to know all public keys of voting *k* members and to perform *k* signature verification for authentication of new member. Also the voting-trust philosophy is different from our straight-delegating situation.

In [9] each node carries its share of private key of certificate authority and each group of *k* nodes is able to reconstruct whole private key and to issue a certificate as well as new secret share for new member. The system is based on threshold cryptography and all nodes in the system act as partial certificate authorities.

Our voucher scheme for Implanted Chain Certificate system described in Section 3 is a combination of both above-mentioned threshold-based schemes [7,9] adapted to requirements of distributed group membership management in ad-hoc networks.

3. VOUCHER SYSTEM

As it was mentioned above the *voucher* is a special issuer of implanted chain certificate. To make a system of IChC effective each voucher needs for vouchership confirmation a single certificate. Therefore for issuing a voucher certificate only one additional key pair is used, the private and public Common Voucher Key (CVK) and each voucher certificate is signed by the private CVK. Private CVK is shared among existing vouchers.

For issuing new voucher the threshold secret sharing and threshold multi-signature protocol are applied. At least *k* existing vouchers with their secret shares, in our case the private CVK, must cooperate to issue a certificate to new voucher as well as its new secret share.

The structure of vouchers can be built in a satisfactory way by using a scheme described in [9]. The scheme is built upon Shamir's threshold secret sharing [10], established on Lagrange interpolation. Any *k* members of the community can recover the secret by Lagrange interpolation, while any less than *k* members of the community reveals no information of the secret [9].

In our scheme in the beginning, the group-key owner establishes at least *k* vouchers and signs their voucher certificates by private CVK. Next the group-key owner distributes to vouchers their secret shares of CVK through a secure channel, e.g. encrypted with each voucher's public key respectively. Thereafter, the group-key owner can erase the private CVK, because apart from the initialization phase, the CVK is never used in whole.

New voucher established by a leader obtains a voucher certificate and a certificate chain from the leader to prove its group membership. Next the voucher has to contact *k* existing vouchers to resign its voucher certificate and so to get single certificate signed by CVK as well as to obtain its new secret share based upon threshold cryptography.

A voucher is established by a leader and it is on the leader's decision, when and why to establish a new voucher. For example, the leader can do this when the cost of verification of its delegation chain is too high, a high number of members have occurred in the area requiring an optimization of the verification process or when there is no answer from an existing voucher till specific time. In our network simulation described in Section 4 we deliberated the last case.

For instance, in Figure 1 a leader L_x issued the voucher certificate to a voucher V_x. Then the voucher V_x connected k (k=3) existing vouchers V_1, V_2, … , V_k and the new V_x voucher was signed by k partial secret shares of V_1, V_2, … , V_k, i.e. the voucher obtained a voucher certificate signed by private CVK. Next the voucher V_x is able to issue an IChC for a chain of certificates.

Our voucher scheme compared to [7,9] does not require connection of *k* authorities for each node. Only a voucher must execute this obligation and only once to confirm its vouchership. A new voucher can spend more time searching and contacting *k* vouchers compared to an ordinary member, the searching process is realized in whole available ad-hoc network. Also the trust of the system is based on a chain of certificates initiating with group-key owner. Moreover, in our scheme the minimum number of contacted existing vouchers as well as the number of all vouchers are tunable parameters. The number of all vouchers can increase whenever necessary during the running of the system.

So far we assume that the new voucher has at least contact to *k* existing vouchers. However, because of node moving it may not always be possible to reach *k* vouchers. In that case it is recommended [9] that requesting entity broadcasts the requests for a limited number of times as well as the requesting node may move to a new location,

where it can find the rest of *k* share holders. Thus node mobility helps provide certification services.

Note that each leader could be a voucher as well, only the voucher certificate has to be issued by the leader to itself and, consequently, the confirmation of vouchership has to be made. Appropriate value of *k* and its effect on voucher system as well as availability of service and number of vouchers in the system are described in further section on the basis of our network simulation results.

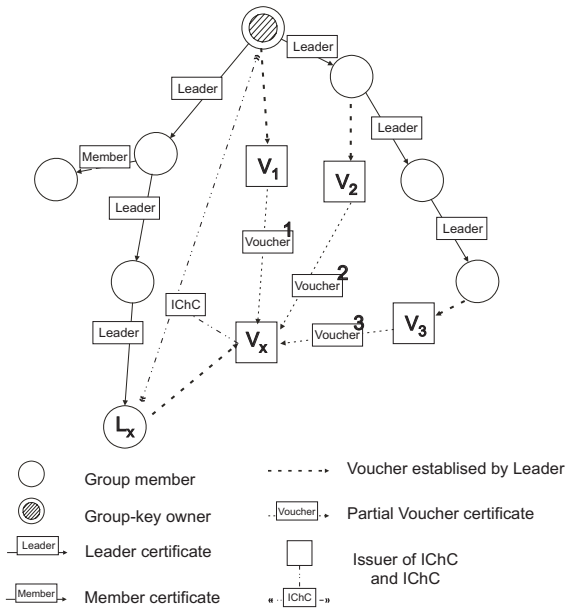

Fig. 1 Voucher System with Implanted Chain Certificate.

4. EVALUATION OF IMPLEMENTATION

This section describes the details of simulation experiments we have carried out to study the performance of the voucher system in ad-hoc network. A variety of workloads and scenarios, as characterized by node mobility and size of the network, were simulated using the network simulator ns2 [11]. For all our simulations we used the 802.11 MAC and physical layer and the built-in radio model that has a radio range of 250 metres. We also used Carnegie Mellon University setdest utility to generate random-way point mobility models with different node moving speed. The speed varies from 0, 1, 3, 5, 10, 15, 20 m/sec. The node speeds 3, 10 and 15 m/sec correspond roughly to low, medium and high mobility [9]. The Random Waypoint mobility model [12] was used. The random path of a mobile node is generated by choosing a destination point at random over the entire area. The mobile node moves towards its own destination along a straight line at a constant random speed. When the destination node is reached, another destination and another speed are generated according to a uniform distribution. The simulations are run with 50 or 100 nodes spread in rectangular two-dimensional area of 1500x1500m^2.

4.1. First set of simulations – Connecting Time

The parameter *k*, the number of contacted vouchers for creating a new voucher, is a tunable parameter. But generally the *k* is chosen in the initialization of the system and it is expensive to change it later. On the other side, if there is a lack of vouchers in the system, a new voucher can be established. Therefore it is important to understand the effects of varying *k* on a given system. The *k* value can range between 1 and *n* (*n* is number of all vouchers created by group-key owner during the initial phase). Setting *k* to a higher value has the effect of making the system more secure against possible adversaries since *k* is the number of vouchers which the adversary needs to compromise to breakdown the system. But at the same time, a higher *k* value makes the service less available since a new voucher needs to contact at least *k* existing vouchers. Therefore, the value *k* should be chosen properly and depends on security policies within the system. It is clear that no value will fit all the systems. Our goal is to investigate the practicability of voucher system for different *k*.

In our simulations, a voucher system comparison of three well-known routing protocols AODV, DSR and DSDV was presented. The ad-hoc protocols are directly supported by the ns2 simulator [11]. A randomly chosen node tries to contact *k* existing vouchers (*k*=1, 3, 5, 10 and 15) in the system for a period of 600 seconds and the time of contacting is gauged. In the current simulation implementation, we use multiple unicasts to simulate a multicast.

Total Number of Mobile Nodes	50 or 100
Number of vouchers	1, 3, 5, 10 and 15
Area of Network	1500m x 1500m
Total Simulation Time	600 seconds
Node Speed (m/sec)	0, 3, 5, 10, 15, 20

Tab. 1 Simulation Parameters for the first set.

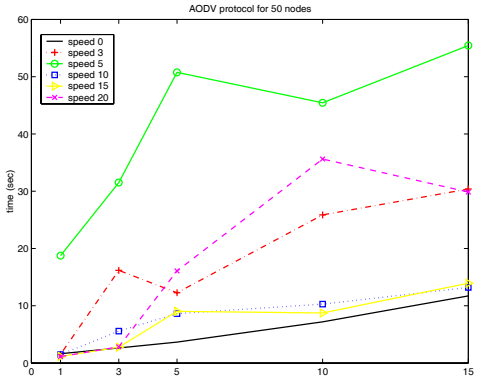

Fig. 2 AODV protocol for 50 nodes.

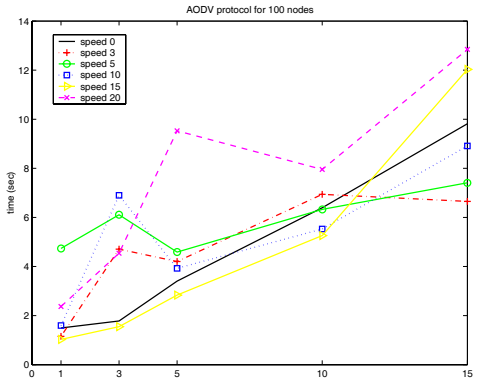

Fig. 3 AODV protocol for 100 nodes.

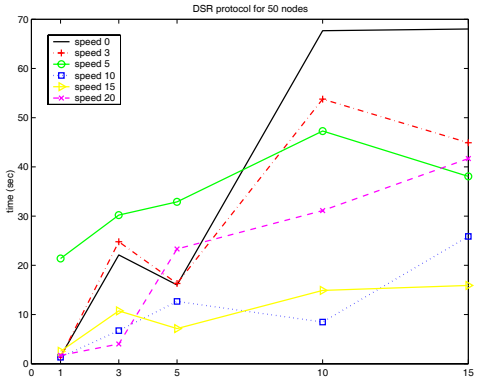

Fig. 4 DSR protocol for 50 nodes.

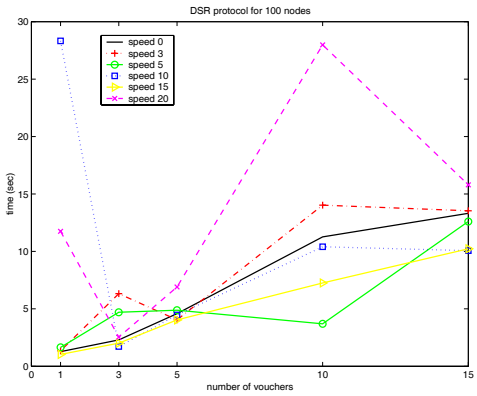

Fig. 5 DSR protocol for 100 nodes.

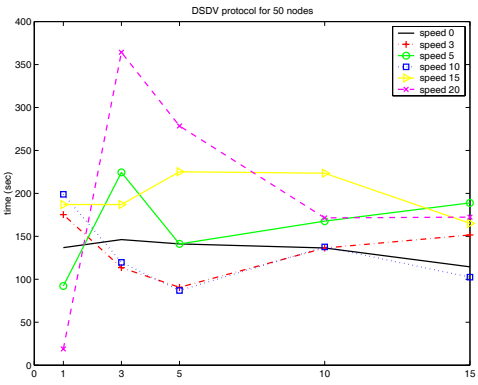

Fig. 6 DSDV protocol for 50 nodes.

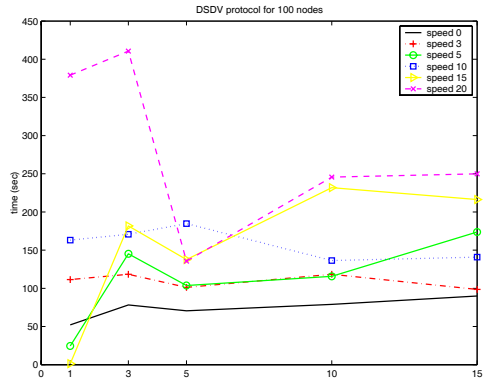

Fig. 7 DSDV protocol for 100 nodes.

The results for different amount of vouchers (k = 1, 3, 5, 10 and 15) are shown in Figure 2, 3, 4, 5, 6 and 7.

From the graphs we note that our algorithm scales well to the network size and node mobility; even for the topology of 50 nodes, high node speed fixed at 20m/sec (72km/h) and large value k=15, the new voucher manages to contact k existing vouchers in less that 400 seconds.

The results for the scenario of 100 nodes are slightly different. As expected, the curves are shifted downwards, since the network density is higher and consequently it requires less time to connect.

From the graphs it is possible to see that all three routing algorithms do perform well. The voucher system with AODV and DSR protocol performs better than DSDV, since reactive routing protocols (AODV, DSR) are more speed-sensitive compared to proactive protocols (DSDV).

The best values were acquired for AODV protocol, where the worst time delay was for speed 20 m/sec, k=15 for 100 nodes smaller than 13 seconds.

The simulations show that it is possible to apply the voucher system in ad-hoc network, even in strong secure system with high k value.

4.2. Second set of simulations – Number of Vouchers

Since the operation of new voucher establishing is prolonged, it is important to set up appropriate number of voucher in the initialization phase. On the other side, if the system is growing, new vouchers are establishing consequentially. Our goal is to detect initial number of voucher system for different scenarios.

In the simulation, only AODV protocol, the best routing protocol for the voucher system is considered. In simulation, a randomly chosen node tries to contact an existing voucher every 5 seconds during 1200 seconds period. If it is not achievable, the process of establishing of a new voucher is inducted. The new voucher has to contact k existing vouchers (k=2) in the system for a period of 60 seconds. The delay time of voucher connecting is set in 100-nodes network to 2 seconds and in 50-nodes network, because of low node density, to 4 seconds.

Total Number of Mobile Nodes	50 or 100
Initial number of vouchers	5
Area of Network	1500m x 1500m
Total Simulation Time	1200 seconds
Node Speed (m/sec)	0, 1, 3, 5, 10, 15, 20

Tab. 2 Simulation Parameters for the second set.

The results are shown in Figure 8, 9 and 10.

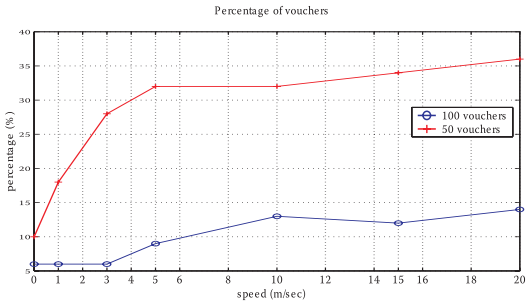

Fig. 8 Percentage of vouchers in the system.

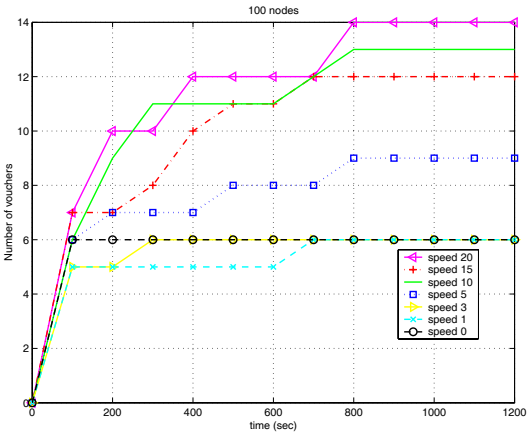

Fig. 9 Number of vouchers for 100 nodes.

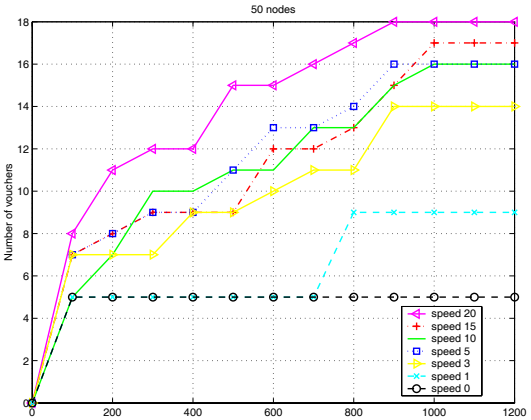

Fig. 10 Number of vouchers for 50 nodes.

From the graph for 100-nodes-simulations, we can see that the number of vouchers ranges from 6 to 14 percent. The higher speed, the higher number of vouchers. An average number of voucher in the 100-nodes system is 10. The system stabilized mostly after 800 seconds.

The results for the scenario of 50 nodes are various. The number of vouchers reaches in extreme speeds up to 36 percent of whole nodes amount. Moreover, the system seems less stabile that for 100 nodes. However, this behaviour of the system is reasonable because of low node density in the network. We can note that the higher the node density, the lower the percentage of needed vouchers. This is because the higher the node density, the higher the probability that multiple paths exist between the source and the destination. In network with low node density, more nodes should be kept awake to maintain the connectivity. Furthermore, the lower speed the lower number of vouchers in system.

In reality, the performance of mobile ad-hoc networks will depend on many factors such as node mobility model, traffic pattern, network topology, radio interference, obstacle positions, and so on. It is difficult to cover all these factors in simulation study. In our simulations we considered the most important factor in performance of ad-hoc networks, which is widely used in most simulation studies, the node mobility. It is clear that it is not possible to incontinently apply the acquired results into each system, but our measurements give a basic insight into the configuration of voucher system as well as confirm that the voucher system is adequate for ad-hoc network scenario.

5. CONCLUSION

In this paper, we presented a practical key management framework for ad-hoc wireless networks for Implanted Chain Certificates Scheme based on vouchers. Vouchers share the responsibility of creating a new voucher for an ad-hoc network using threshold cryptography. Each voucher is responsible for issuing an IChC in the system.

We develop an efficient and effective communication system for mobile nodes to correspond with vouchers based on combination of protocols in [7,9]. Our simulation results show the effectiveness of our approach. Further we provide some insights into the configuration of such security services in ad-hoc networks as well as we suggest, based on our simulations of the voucher system among mobile nodes, an appropriate number of vouchers.

REFERENCES

[1] Johnson, D. B., Maltz, D. A., Hu, Y. Ch.: "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)," Internet Draft, IETF Mobile Ad hoc Networks (MANET) Working Group, 2004.

[2] Perkins, C. E., Belding-Royer, E. M., Das, S. R.: "Ad hoc On-Demand Distance Vector (AODV) Routing," Internet Draft, IETF Mobile Ad hoc Networks (MANET) Working Group, 1999.
[3] Perkins, C., Bhagwat, P.: "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," in Proc. ACM SIGCOMM'94, London, UK, 1994.
[4] Huraj, L., Reiser, H.: "Efficient Verification of Delegation in Distributed Group Membership Management." IFIP TC11/WG11.3 Eighteenth Annual Conference on Data and Applications Security; Sitges, Catalonia, Spain, July 2004.
[5] Aura, T., Mäki, S.: "Towards a survivable security architecture for ad-hoc networks." In Proc. Security Protocols, 9th International Workshop, volume 2467 of LNCS, p. 63-79, Cambridge, UK, April 2001.
[6] Mäki, S., Aura, T., Hietalahti, M.: "Robust Membership Management for Ad-hoc Groups." In Proceedings of the 5th Nordic Workshop on Secure IT Systems, NORDSEC 2000, Reykjavik, Iceland, 2000.
[7] Yi, S., Kravets, R.: "MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks", 2nd Annual PKI ResearchWorkshop Program (PKI 03), Gaithersburg, Maryland, April, 2003.
[8] Pathak, V., Iftode, L.: "Byzantine fault tolerant authentication" Technical Report, Dept of Computer Science, Rutgers University, 2003.
[9] Kong, J., Zerfos, P., Luo, H., Lu, S., Zhang, L.: "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks," International Conference on Network Protocols (ICNP), pp. 251–260, 2001.
[10] Shamir, A.: "How to Share a Secret." Communications of the ACM, 22(11), p. 612-613, November 1979.
[11] The Network Simulator – ns-2. Available on: http://www.isi.edu/nsnam/ns/.
[12] Broch, J., Maltz, D. A., Johnson, D. B., Hu, Y. Ch., Jetcheva, J.: "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols," in Proc. MobiCom'98, Dallas, TX, Oct. 1998.

BIOGRAPHY

Ladislav Huraj was born on 3.1.1974. He received the MSc. degree at the Faculty of Mathematics and Physics, Comenius University, Bratislava, Slovakia in 1997. He is currently a Ph.D. student at the Faculty of Informatics and Information Technologies, Slovak Technical University in Bratislava. He is a senior lecturer at the Dept. of Computer Science, Faculty of Natural Sciences, Matthias Bel University in Banská Bystrica since 1997. His research interests include IT and network security, certification systems as well as methodology of cryptology teaching.