**Advances in Science and Technology Research Journal**
Volume 8, No. 22, June 2014, pp. 12–18
DOI: 10.12913/22998624.1105141

*Research Article*

# AUTHENTICATION ARCHITECTURE USING THRESHOLD CRYPTOGRAPHY IN KERBEROS FOR MOBILE AD HOC NETWORKS

**Hadj Gharib[1], Kamel Belloulata[2]**

[1] Mathematics laboratory, Djillali LIABES University, Sidi Bel Abbes, Algeria, e-mail: gharib2@gmail.com

[2] RCAM laboratory, Djillali LIABES University, Sidi Bel Abbes, Algeria, e-mail: k_belloulata@yahoo.fr

Received: 2014.03.07
Accepted: 2014.05.20
Published: 2014.06.05

**ABSTRACT**

The use of wireless technologies is gradually increasing and risks related to the use of these technologies are considerable. Due to their dynamically changing topology and open environment without a centralized policy control of a traditional network, a mobile ad hoc network (MANET) is vulnerable to the presence of malicious nodes and attacks. The ideal solution to overcome a myriad of security concerns in MANET's is the use of reliable authentication architecture. In this paper we propose a new key management scheme based on threshold cryptography in kerberos for MANET's, the proposed scheme uses the elliptic curve cryptography method that consumes fewer resources well adapted to the wireless environment. Our approach shows a strength and effectiveness against attacks.

**Keywords:** authentication, attacks, Kerberos, MANET, threshold cryptography.

## INTRODUCTION

### Background

A mobile ad hoc network is formed by a population of wireless nodes without preexistent network infrastructure or central administration. This nature makes it easy to deploy especially in environments where it's difficult to implement a regular network. MANET networks can be used in both civilian and military applications where security of exchanges must be ensured.

### Motivation

User authentication is an important security measure to protect confidential data. Without a way to check a user, data access can be granted to users or groups which are not normally allowed. If the number of nodes is small, an authentication node to node is relatively easy to implement, but if the number of nodes becomes large, a total security strategy must be carefully implemented. The introduction of a Trusted Third Party (TTP) is highly recommended. Pirzada and McDonald in [1] used a TTP based on Kerberos, which inspired our idea. Although this model is widely used, it has inherited all the weaknesses of the Kerberos authentication system [2], such as guessing and replay attacks; but the most important is the presence of a single point of failure, it requires continuous availability of a central server. When the Kerberos server is down, no one can log in. This can be mitigated by using an improved distribution of authentication servers using threshold cryptography on elliptic curves that produces less computation which is well suited to MANETs.

### Related work

Secret sharing scheme was first introduced by Shamir in [3] and now widely used in many cryptographic protocols as a tool for securing information [4, 5, 6, 7, 8, 9, 10]. Zhou et al. in [4] proposed the use of threshold cryptography for providing security to Ad-Hoc networks and enumerate challenges in the design of such a scheme. In [5] Azer et al. describes a survey on the authentication technique based on the same principle and also described some challenges to take into account. In [6] Govindan and Mohapatra present a detailed survey on various trust computing approaches that are geared towards MANETs. A distributed key management and authentication approach by deploying the concepts of identity-based cryptography and threshold secret sharing was proposed in [7]. In [8] RSA-threshold cryptography-based scheme for MANETs using verifiable secret sharing (VSS) scheme is presented. Another scheme presented in [9] proposes a fully distributed public key certificate management system based on trust graphs and threshold cryptography. In [10] the authors use a threshold Signature in Anonymous Cluster-Based MANETs. However none of the above works use kerberos [11] as TTP in threshold cryptography in MANETs. To the best of our knowledge, our proposed security architecture is the first in which the authentication is based on the distribution of Kerberos TGS combined with threshold cryptography in mobile ad hoc networks (MANETs).

### Challenging issues

The main vulnerability of MANETs comes from their open architecture. Unlike wired networks that have dedicated routers, each mobile node in an ad hoc network can function as a router and forwards packets for other nodes [12]. The wireless channel is accessible to both legitimate network users and malicious attackers. The security of wireless networks is sensitive to a series of non-existent problems in wired networks, in wireless networks, data flows in the air, which makes it easy to sniff by eavesdroppers who can inject malicious messages. Wireless networks also have fuzzy boundaries difficult to control. Wireless devices in the network can be the target of physical attacks. Consequently, the secrets and sensitive data could be extracted. The computational capacity of a mobile node is also a constraint as the node can hardly perform computationally intensive tasks as asymmetric cryptographic calculation due to the limited energy resources of the batteries.

The network topology is very dynamic as nodes frequently join and leave the network. The wireless channel is also subject to interference and errors which affect the bandwidth and delay. Despite such dynamics, mobile users may request for anytime, anywhere security services as they move from one place to another.

Security solution must take into account all these aspects for the performance and quality of service desired.

The ideal solution must take into account:

- The collaboration of all mobile nodes is involved in thwart attacks.
- The solution must extend across all layers of networks each layer contributing to a line of defense.
- Security solution must thwart internal and external threats.
- Finally and most importantly, the security solution must be feasibly adapted to the network to be secured.

### Organization

The rest of the paper is organized as follows: First we present a brief overview of the Kerberos authentication system and ElGamal threshold cryptosystem. Then, we present our proposed model with security analysis. Finally, we compare our proposal with threshold-RSA based schemes.

## PRELIMINARIES

### The Kerberos authentication protocol

Kerberos is a network authentication protocol created by MIT utilizing a symmetric key cryptography to authenticate users to network services. Kerberos uses tickets instead of passwords, thus avoiding the risk of fraudulent interception of users' passwords.

**Kerberos credentials.** Kerberos has two types of credentials: tickets and authenticators. A ticket is used by a user to authenticate itself to a server from which it requests a service, it contains the server ID (Identifier), the user ID, a timestamp, a lifetime, and a session key encrypted by the authentication server key. An authenticator is used to prevent replay attacks. Generally, an authenticator contains the user's ID and a timestamp encrypted with a session key shared between the user and the authentication server.

**Kerberos exchanges.** The Kerberos protocol consists of three exchanges: the authentication server (AS), the Ticket Granting Service (TGS) and the application server (AP). The AS exchange allows the client to obtain credentials to prove his identity at TGS. The TGS exchange allows the client to authenticate itself to the TGS and obtain

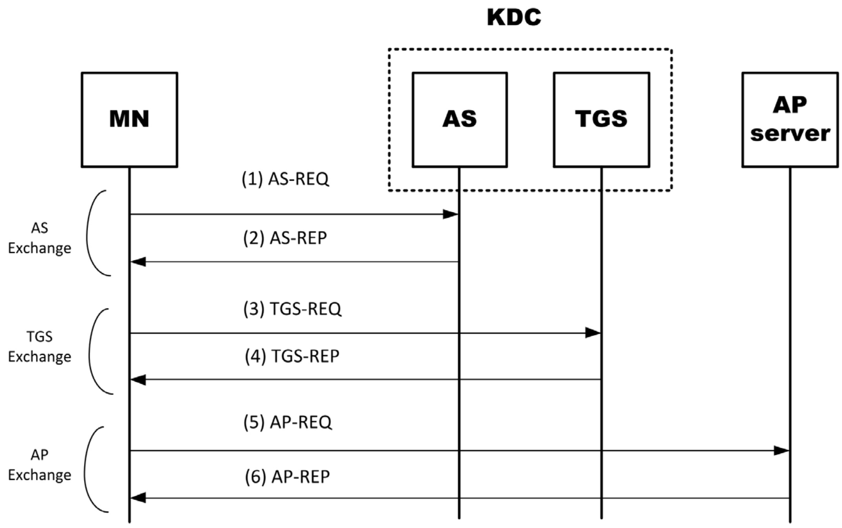



**Fig. 1.** The Kerberos protocol exchanges

a service ticket for the desired service. AP exchange is performed between the client and the service to authenticate the client before granting access to resources (Figure 1).

## Shamir's Secret Sharing

Secret sharing refers to methods for distributing a secret among a group of participants (also called shareholders), each of which is assigned a share of the secret. The secret can be reconstructed if a sufficient number of shares are combined. In the *(k, n)* threshold secret sharing, the secret is distributed to *n* shareholders, and any *k* out of these *n* shareholders can reconstruct the secret, but any collection of less than *k* partial shares can't get any information about the secret [13].

**Description.** Dealing phase:

- Let $s$ be a secret from some $Zp$, $p$ prime
- Select a random polynomial

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots f_{k-1} x^{k-1}$$

under the condition that $f(0) = s$:

- Select $f_1, \ldots, f_{k-1} \leftarrow R\ Zp$ randomly
- Set $f_0 \leftarrow s$
- For $i \in [1, n]$, distribute the share $s_i = (i, f(i))$ to the $i^{\text{th}}$ party

The secret $s$ can be reconstructed from every subset of $k$ shares by the Lagrange formula,

Given $k$ points $(x_i, y_i)$, $i = 1, \ldots, k$,

$$f(x) = \sum_{i=1}^{k} y_i \prod_{j=1, j\neq i}^{k} \frac{x - x_j}{x_i - x_j} (mod\, p)$$

and

$$s = f(0) = \sum_{i=1}^{k} y_i \prod_{j=1, j\neq i}^{k} \frac{-x_j}{x_i - x_j} (mod\, p)$$

Any subset of up to $k$–1 shares does not leak any information on the secret.

## Elliptic Curve ElGamal threshold cryptosystem

ElGamal cryptosystem is based on the difficulty of solving the discrete logarithm problem [14]. We'll assume that we have a Trusted Third Party (*TTP*) – Kerberos in our case – that sets up the system.

**Phase 1**: Key generation for $(t, n)$

- Choose a large prime: $a$ prime $p$ such that $p = 2q + 1$, $q$ also prime.
- Find a generator $g$ of order $q$.
- Choose a random $a \in \mathbb{Z}q$ and compute $y = \beta^x$.
- Compute a random degree $t - 1$ polynomial

$$f(x) = a + \sum_{j=1}^{t-1} a_i x^i \ mod\ p$$

The $a_i$ are chosen randomly.

- Compute $n$ shares of $a$: $s_i = f(x_i)$ for each user $i$.

The public key is $pk = (p, g, \beta)$ and the master private key is $sk = (x)$. The master private key is not given to anyone.

**Phase 2**: Encryption

- Choose a random $k \in \mathbb{Z}q$ and compute $c_1 = g^k \ mod\ p$.
- Compute $c_2 = m\beta^k \ mod\ p$.
- The ciphertext is:

$$c = (c_1, c_2) = (g^k, m\beta^k).$$

**Phase 3**: Decryption

To decrypt a ciphertext $c = (c_1, c_2)$, $t$ participants must ask the *TTP* for their decryption shares for this ciphertext.

*TTP* compute $d_i = c_1^{s_i} = \left(g^k\right)^{s_i} mod\ p$, for each user $i$ that asks for decryption share.

Suppose that $I$ is the set of $t$ participants that requested a decryption share . Once each user has their decryption share $d_i = g^{ks_i} = g^{kf(x_i)}$, the users cooperate to compute:

$$d = \prod_{i\in I} d_i^{\Lambda_i} \equiv \prod_{i\in I} \left(g^{kf(x_i)}\right)^{\Lambda_i} \equiv \prod_{i\in I} g^{kf(x_i)\Lambda_i} \equiv g^k \sum_{i\in I} f(x_i)\Lambda_i \equiv g^{kf(0)} \equiv g^{ka} (mod\, p).$$

The participants must cooperate so that can

- Compute the $\Lambda_i$ values, and
- Compute $g^{ka}$.

The plaintext is computed as [15]:

$$m = c_2 d^{-1} = \left(m\beta^k\right)\left(g^{ka}\right)^{-1} = mg^{ka}g^{-ka} = m\ mod$$

**Phase 4**: Elliptic Curve ElGamal Threshold

This operation can be done by converting message to a point on an elliptic curve and vice-versa using the Koblitz's method [16, 17].

**Phase 5**: Finally, we use the Lagrange interpolation formula to recover the message.

**Table 1.** Notations used in this paper

| Notations | Descriptions |
|---|---|
| *MN* | Mobile Node |
| *AS* | Authentication Server |
| *TGS* | *Ticket-Granting Server* |
| $ID_x$ | Identity of *x* |
| $TKT_x$ | Ticket *x* |
| $T^i$ | Timestamp *i* = ',",''',"",''''' |
| $E_k$ | Encryption by using key |
| $K_{x,y}$ | The shared key between *x* and *y* |
| $AUTH_{x,y}$ | Authenticator between *x* and *y* |

## OUR PROPOSAL

Mobile node sends resource ticket and authenticator to the service encrypted with the MN/AS key (pre-distributed via a secure channel in the registration phase). The AS confirms the identity of MN, if valid, it responds back to MN with a modified version of timestamp in the authenticator encrypted with MN/AS key. In this phase instead of using only one TGS, we use the ECC-ElGamal Threshold Cryptosystem to divide TGS into multiple parts to allow threshold authentication, it means one TGS cannot ensure the completion of the authentication process without the participation of a number predefined of TGS.

Algorithm: **Distributed TGS**

1- $MN$ sends $TGT$ request to $AS$

$$MN \rightarrow AS: ID_{MN} \parallel ID_{TGS} \parallel T'$$

2- $AS$ *grants* a $TGT$ to $MN$ and if $ID_{MN}$ *valid continue else reject request*

$$AS \rightarrow MN: ID_{MN} \parallel TKT_{TGS} \parallel E_{kMN}[K_{MN,TGS} \parallel T'' \parallel ID_{TGS}]$$

$$TKT_{TGS} = E_{KTGS}[K_{MN,TGS} \parallel ID_{MN} \parallel T'' \parallel ID_{TGS}]$$

$Repeat$

{ $\quad k: (Number\ of\ TGS)$

3- $MN \rightarrow TGS: ID_{AP} \parallel TKT_{TGS} \parallel AUTH_{MN,TGS}$

$$AUTH_{MN,TGS} = E_{K(MN,TGS)}[ID_{MN} \parallel T''']$$

4- $TGS \rightarrow MN: ID_{MN} \parallel TKT_{AP} \parallel E_{K(MN,TGS)}[K_{MN,AP} \parallel T'''' \parallel ID_{TGS}]$

$$TKT_{AP} = E_{KAP}[K_{MN,AP} \parallel ID_{MN} \parallel ID_{AP} \parallel T'''']$$

5- $MN \rightarrow AP: TKT_{AP} \parallel AUTH_{MN,AP}$

$$AUTH_{MN,AP} = E_{K(MN,AP)}[ID_{MN} \parallel T''''']$$

6- $AP \rightarrow MN: E_{K(MN,AP)}[T''''']$

$k = k + 1$

$until\ k = r\ (r: the\ min\ of\ shareholders)$

$k < n\ (n: number\ total\ of\ TGSs)$

### Details of the proposal description

1. The *MN* (Mobile Node) asks for a *TGT* (Ticket Granting Ticket), the *MN* send a message to the *AS* requesting services, which includes the *MN ID* and *TGT ID*.
2. The *AS* grants a *TGT* to *MN*. The *AS* will check the *MN's ID*. If the *MN* is valid, the *AS* create a *TGT Ticket tgs* and generate a Session key $K_{MN,TGS}$ encrypted by the *MN* key $K_{MN}$ to protect communication between *MN* and *TGS*, and send all this to *MN*. The *Ticket TGS* includes *MN ID*, the *TGS ID* – of *shareholders TGS* – timestamp, ticket validity period, and the $K_{MN,TGS}$ session key. The $K_{MN}$ is only known by the *MN* and the *AS*.
3. After receiving the message from *shareholders TGS*, the *MN* decrypts the message to obtain the *Ticket TGS* and $K_{MN,TGS}$. When asking for a *Ticket AP*, the *MN* must send a request message to *TGS*, which includes *AP's ID*, the *Ticket TGS* and the encrypted authenticator $AUTH_{MN,TGS}$ by using $K_{MN,TGS}$.
4. *Shareholders TGS* grant *Ticket AP* to *MN*. Upon receiving the *MN's* request message, the *TGSs* decrypts *Ticket TGS* using its own secret key to get $K_{MN,TGS}$, then uses it to decrypt $AUTH_{MN,TGS}$, thus it can confirm the *MN* through the decrypted message and if the operation is right they generate a session key $K_{MN,AP}$ for the communication service between *MN* and the *AP*, then create a *Ticket AP*, which includes *MN's ID*, *AP's ID*, new timestamp, *Ticket AP* validity period and $K_{MN,AP}$. Then *TGS* encrypts *Ticket AP* using $K_{AP}$ and session key $K_{MN,AP}$ using $K_{MN,TGS}$ and sends them to *MN* which can decrypt the replay message by using $K_{MN,TGS}$ to obtain *Ticket AP* and $K_{MN,AP}$.
5. The *MN* forwards the *Ticket AP* to the application server with a new authenticator $AUTH_{MN,AP}$.
6. *AP* decrypts *Ticket AP* and $AUTH_{MN,AP}$ separately, and judges whether the requests is effective by comparing the all containing information and more precisely the timestamps to prevent a replay attack.

### Advantage of our proposed architecture

Our scheme ensures the availability of the service; in traditional kerberos the KDC is single point of failure, by dividing the TGS into n parts and at least k parts are need to achieving the authentication operation, doing this we provide a deterministic security guarantees. Besides these, our ECC-TC architecture can provide equivalent security with shorter processing time and smaller key size [18] (Table 2).

**Table 2.** Key sizes in bits for equivalent levels

| RSA | Elliptic Curve |
|---|---|
| 1024 | 160 |
| 2048 | 224 |
| 3072 | 256 |

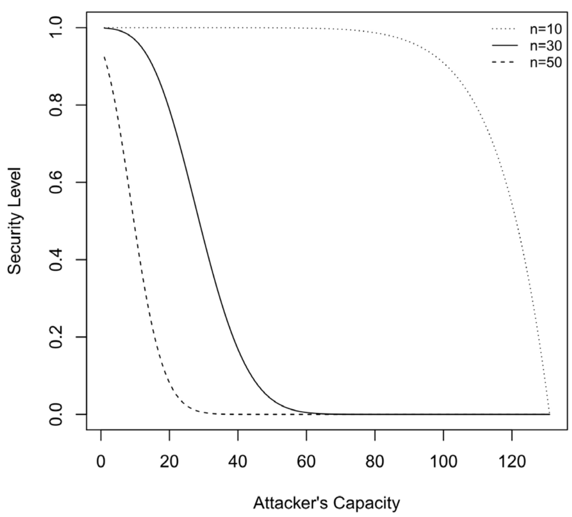
## ANALYSIS

### Measuring the security level for distributed TGSs

Assuming the distributed TGS nodes are anonymous and an adversary cannot discover their identity, the best approach for the adversary is to compromise as many nodes as possible in a given amount of time, hoping that enough TGS nodes are included among the compromised nodes. The following equation captures this situation [19], which was simulated with the R language [20] (Figure 2):

$$Security\ Level = 1 - \frac{\sum_{c}^{i=k}\binom{n}{i}\binom{M-n}{c-i}}{\binom{M}{c}}$$

Emphasize that if the difference between *n* and *k* is too large, the system security is deteriorating.




Varying *n* (*k* = 10)

**Fig. 2.** Security level

### Computational complexity

The computations in our proposal depend on key generation and operations such as encryption, decryption, distribution and verification. The master key generation uses threshold secret sharing, and the computational complexity comes from the number of shareholders.

### Processing time

According to the results presented in [21, 22, 23]. It is very clear that the use of elliptic curves cryptography is very suitable for wireless environments, as shown in Figure 3. At the 192-bit ECCEG-TC is roughly 2 to 3 times as fast as an 1024-bit RSA private key operation which is higher than the required security level security level (Table 2).

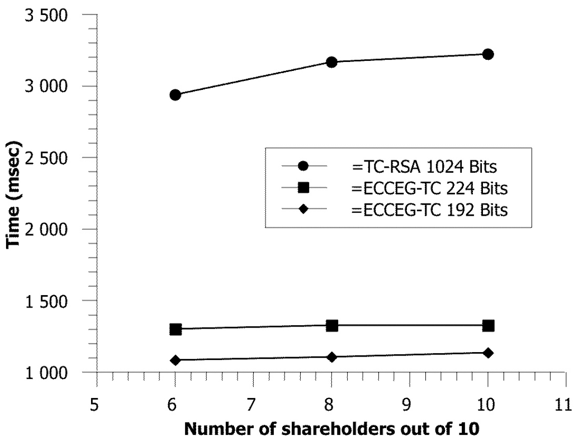



**Fig. 3.** Processing time

### Guessing attacks prevention

Our system is resistant to guessing attacks, the introduction of encrypted timestamps in exchanged messages, make the task difficult for an attacker trying to enter guessed passwords. [24, 25, 26, 27].

### Replay attack prevention

We use a synchronized timestamp embedded in the message within acceptance time window to prevent replay attack; this countermeasure ensures the freshness of messages in a session.

## CONCLUSION

It has been demonstrated that the use of RSA based authentication scheme in wireless environments is not preferable. The proposed authentication scheme based on Elliptic curve ElGamal threshold cryptosystem offers both availability and strong security level required in mobile Ad hoc networks and has proven to be a best method for resistance at offline guessing attack and reply attack. By using elliptic curve cryptography, our scheme is efficient to be implemented in mobile devices. Future work focuses on validation of our study by simulations.

## REFERENCES

1. Asad A., Pirzada McDonald C., Kerberos Assisted Authentication in Mobile Ad-hoc Networks. In: CRPIT ’04 Proceedings of the 27th conference on Australasian computer science, Vol. 56, 41–46, Australian Computer Society, Inc., 2004.
2. Bellovin S.M., Merritt M. Limitations of the Kerberos authentication system. ACM SIGCOMM Computer Communication Review, vol. 20(5), 1990, 119-132.
3. Shamir A. How to share a secret. Communications of the ACM, Vol. 22(11), 1979, 612-613.
4. Zhou L. and Haas Z.J., Securing Ad Hoc Networks. IEEE Network., vol. 13, 1999, 24-30.
5. Azer M.A., El-Kassas S.M. and El-Soudani M.S. Threshold cryptography and authentication in ad hoc networks survey and challenges. In: Systems and Networks Communications, ICSNC 2007. IEEE Second International Conference on, p. 5.
6. Govindan K. and Mohapatra P. Trust computations and trust dynamics in mobile adhoc networks: a survey. Communications Surveys & Tutorials, IEEE, 14(2), 2012, 279-298.
7. Deng H., Mukherjee A., and Agrawal D.P. Threshold and identity-based key management and authentication for wireless ad hoc networks. In: Information Technology: Coding and Computing, Proceedings. ITCC 2004. IEEE International Conference on, p. 107-111.
8. Sarkar S., Kisku B., Misra S., Obaidat M.S. Chinese Remainder Theorem-Based RSA-Threshold Cryptography in MANET Using Verifiable Secret Sharing Scheme. Wireless and Mobile Computing, Networking and Communications. WIMOB 2009. IEEE International Conference on, p. 258-262.
9. Omar M., Challal Y., and Bouabdallah A. Reliable and fully distributed trust model for mobile ad hoc networks. Computers & Security, 28(3), 2009, 199-214.
10. Park Y. and Moon S. Anonymous cluster-based MANETs with threshold signature. International Journal of Distributed Sensor Networks, Article ID 374713, 9 pages, 2013.

11. Neuman T.Y., Hartman S., and Raeburn K. The Kerberos Network Authentication Service (V5). RFC 4120, July 2005.
12. Yang Hao, Luo Haiyun, Ye Fan, et al. Security in mobile ad hoc networks: challenges and solutions. Wireless Communications, IEEE, vol. 11(1), 2004, 38-47.
13. Dey H. and Datta R. A threshold cryptography based authentication scheme for mobile ad-hoc network. In: Advances in Networks and Communications. Springer Berlin Heidelberg, 2011. p. 400-409.
14. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. Information Theory, IEEE Transactions on, vol. 31, 1985, p. 469-472.
15. https://www.scs.carleton.ca/sites/default/files/course_page/secretsharing.pdf, Last accessed: 14-02-2014.
16. Koblitz N. A Course in Number Theory and Cryptography (Graduate Texts in Mathematics, No 114), Springer-Verlag, 1994.
17. Padma B.H., Chandravathi D. and Roja P. Prapoorna. Encoding and decoding of a message in the implementation of Elliptic Curve cryptography using Koblitz's method. International Journal on Computer Science and Engineering, vol. 2(5), 2010.
18. http://www.nsa.gov/business/programs/elliptic_curve.shtml, Last accessed: 27-01-2014.
19. Yi Seung and Kravets R. MOCA: Mobile certificate authority for wireless ad hoc networks. In: 2nd Annual PKI Research Workshop Program (PKI 03), Gaithersburg, Maryland 2003, p. 3-8.
20. http://www.r-project.org/ Last accessed: 02-03-2014.
21. Ertaul L., and Chavan N.J. RSA and Elliptic Curve-ElGamal Threshold Cryptography (ECCEG-TC) Implementations for Secure Data Forwarding in MANETs. Threshold, vol. 7(8), 2007, p. 9.
22. Ertaul L. and Lu Weimin. ECC based threshold cryptography for secure data forwarding and secure key exchange in MANET (I). In: NETWORKING 2005. Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications Systems. Springer Berlin Heidelberg, 2005, 102-113.
23. Lauter K. The advantages of elliptic curve cryptography for wireless security. Wireless Communications, IEEE, vol. 11(1), 2004, 62-67.
24. Li Chun-Ta and Chu Yen-Ping. Cryptanalysis of Threshold Password Authentication Against Guessing Attacks in Ad Hoc Networks. IJ Network Security, vol. 8(2), 2009, 166-168.
25. Corin R., Malladi S., Alves-Foss J., et al. Guess what? Here is a new tool that finds some new guessing attacks. Twente Univ. Enschede (Netherlands), Dept of Computer Science, 2003.
26. Chai Zhenchuan, Cao Zhenfu and Lu Rongxing. Threshold password authentication against guessing attacks in ad hoc networks. Ad Hoc Networks, vol. 5(7), 2007, 1046-1054.
27. Ruan Na, Nishide Takashi and Hori Yoshiaki. Elliptic curve ElGamal Threshold-based Key Management Scheme against Compromise of Distributed RSUs for VANETs. Journal of Information Processing, vol. 20(4), 2012, 846-853.