Editor in Chief Dr Wei WANG

International Journal of Security (IJS)

Book: 2009 Volume 3, Issue 1
Publishing Date:28-02-2009
Proceedings
ISSN (Online): 1985-2320

IJS Journal is a part of CSC Publishers
http://www.cscjournals.org

Published in Malaysia

Typesetting: Camera-ready by author, data conversation by CSC Publishing Services – CSC Journals, Malaysia

CSC Publishers

Table of Contents

Volume 3, Issue 1, January/February 2009.

Pages

Identity-Based Key Management in MANETs using Public Key Cryptography

Dr. Anil Kapil anil_kdk@yahoo.com
Professor, M M Institute of Computer Technology and Business Management, M M University, Mullana, Ambala, Haryana, India

Mr. Sanjeev Rana sanjeevrana@rediffmail.com
Asst. Professor, Department of Computer Engineering, M M Engineering College, M M. University, Mullana, Ambala, Haryana, India

ABSTRACT

Wireless mobile Ad Hoc Networks (MANETs) are an emerging area of mobile computing. MANETs face serious security problems due to their unique characteristics such as mobility, dynamic topology and lack of central infrastructure support. In conventional networks, deploying a robust and reliable security scheme such as Public Key Infrastructure (PKI) requires a central authority or trusted third party to provide fundamental security services including digital certificates, authentication and encryption. In the proposed scheme, a secure identity-based key management scheme is proposed for networks in environments without any PKI. This scheme solved the security problem in the MANET and is also suitable for application to other wired network structures.

Keywords: MANETs, Key Management, Key Distribution

1. INTRODUCTION

1.1 Overview

The demand for more flexible, easy to use and advanced wireless communication technologies has provided opportunities for new networking technologies. MANETs are an innovative approach to a new form of wireless networking technology. There are several issues, such as routing, scalability, quality of service and security that need to be solved before implementing these network technologies in practice. Most of the research that has been done on ad hoc networking has faced on routing [1] [2] [3]. Other issues such as security and network addressing have received considerably less attention [4] [5]. Designing and implementing any kind of security scheme requires a secret to set up a trust relationship between two or more communicating parties. For example, the ability of node A to trust node B could be achieved by a process that permits node A to verify that node B is genuine to a set of pre-imposed rules. This in turn could be achieved by permitting such genuine node to establish authenticated shared secrets that other nodes cannot. The process of establishing such authenticated shared secrets could be achieved by a suitable key management scheme. The fundamental security services provided by every key management system are key synchronism, secrecy, freshness, independence, authentication, confirmation and forward and backward secrecy [6]. Conventional key management techniques may either require an online trusted server or not. The infrastructureless nature of MANETs precludes the use of server based protocols such as Kerberos [7]. There are two intuitive

symmetric-key solutions, though neither is satisfactory. The first one is to preload all the nodes with a global symmetric key, which is vulnerable to any point of compromise. If any single node is compromised, the security of entire network is breached. Another solution is to let each pair of nodes maintain a secret that is known to those two nodes. This approach suffers from three main drawbacks.

- First, as the size of network increases, securely updating the overall n(n-1)/2 keys in the network is not an easy task.
- Second, each node requires storing (n-1) keys, which may cause significant overhead in a large network.
- Last, there is a problem of scalability because it is difficult to establish pairwise symmetric keys between existing nodes and newly joined node.

Symmetric key techniques are commonly criticized for not supporting digital signatures because each key is known to only two nodes. This renders public key solutions more appealing for MANETs, which is used in this paper.

To address these security related issues, this paper present a proposed scheme using ID-based cryptography approach for key management and key distribution and also provides end-to-end authentication without any PKI. This paper is organized into four sections. This next section gives the overview of existing approaches. It also presents the benefits of our scheme and limitation of the existing schemes. Section two presents our proposed ID-based key management scheme for mobile ad hoc networks. Section three explains the security analysis of various attacks on the proposed scheme. Section four presents conclusion and future works.

1.2 Related Works

Recent researches have shown that wireless ad hoc networks are highly vulnerable to various security threats due to their inherent characteristics [8] [9]. This leaves ad hoc key management and key distribution as a wide open problem. There has been a rich literature on public key management in MANETs, [10] [11] [12] [13] [14] [15]. These schemes all depend on certificate-based cryptography (CBC), which uses public key certificates to authenticate public keys by binding public keys to the owner's identities. A main concern with CBC-based approaches is the need for certificate-based public key distribution. Another approach is to preload each node with all others public key based certificates prior to network deployment. This leads not only the problem of scalability when network size increases, but also difficult to update keys in a secure and cost effective fashion. One new approach is about on-demand certificate retrieval may cause both unfavorable communication latency and communication overhead. As a powerful alternative to CBC, ID-based cryptography (IBC) has been gaining momentum in recent years. The idea of Identity based cryptosystem was first proposed by Shamir [15] to simplify the conventional public key cryptosystem, and make the key management easier [16]. Khalili, et. al proposed a protocol for management and authentication in an ad hoc network that is based on an ID-based scheme in [17].

It allows public keys to be derived from entities known identity information, thus eliminating the need for public key distribution and certificates. This featured inspired a few IBC-based certificateless public key management schemes for MANETs such as [17] [18][19][20]. The basic idea is to let some [17] [18] [20] or all network nodes called a shareholders, share a network master-key using threshold cryptography [21] [22] and collaboratively issue ID-based private keys. There, however, remain many issues to be satisfactorily resolved:

- First of all, all the security of the whole network is breached when a threshold number of shareholders are compromised.
- Second, updating ID-based public/private keys requires each node to individually contact a threshold number of shareholders, which represents a significant overhead in large scale MANET.

To address these security related issues, this paper present a proposed scheme using Identity based cryptography using public key cryptography approach for key management. The main benefits of the proposed scheme are:

- This scheme does not need any inline Certification Authority to share secret key.

- The scheme avoids the need for users to generate their own public keys and to then distribute these keys throughout the network.
- There is no need to handle heavily used public key cryptography based certificates

2. THE PROPOSED SCHEME

In this section, a secured ID-based key management scheme is proposed suitable for applying in wireless mobile ad hoc network. Similar to other ID-based cryptosystems, a trusted key generation center is needed in this scheme for verifying user identity and generating the corresponding private keys. After all users have registered, the key generation center can be closed or off-line. The proposed scheme consists of four phases: initialization, registration of user, verification of user, and key exchange between two users as shown in figure 1.

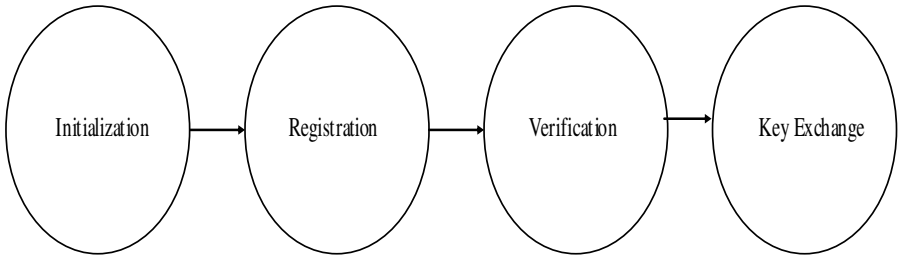


FIGURE 1: Four phases of Key Exchange process in Proposed Scheme

The proposed scheme used some notation given below in table 1.
Let U = {U_1, U_2, U_3, … U_N} are different users and ID = {ID_1, ID_2, ID_3, …. ID_N} be the identity (which is unique) of respective users in the mobile ad hoc network. Each user U_i has a unique identity ID_i, which is known to all the other users. Each user can execute the scheme multiple times with different partners. This is modeled by allowing each user an unlimited number of instances with which to execute the scheme.

TABLE 1: Notation

p & q	Two large and strong prime numbers
n	Product of p and q
ϕ (n)	Product of (p-1) and (q-1)
e	Integer number prime with respect to n
d	Part of private key of Key Center and is equal to e^{-1} mod ϕ (n)
ID_i, ID_j	Identity of users U_i and U_j
n,e	Pair used as public key of key distribution center
n,d	Pair used as private key of key distribution center
T_i , T_j	Time stamp used by users U_i and U_j
h( )	One-way hash function
g_i, g_j	Encrypted code of ID_i and ID_j of users U_i and U_j respectively created by Key Center
r_i, r_j	Large random numbers chosen as secret by users U_i and U_j respectively
SK_i , SKj	Secret session key established at user U_i and U_j

Initialization phase: In this phase, each user U_i ε U gets his long-term public and private keys. The key generation center randomly chooses a secret key as master key and then computes, and publishes corresponding public key. To construct this private-public key pair, we are motivated by the RSA [23] scheme, the key generation center calculates public key (n, e) and private key (p, q, d, ϕ(n)). In addition, the center also determines a primitive element α in both of the fields GF(p)

and GF(q), and chooses a one-way hash function h( ). Similarly, treat (α, h( )) along with (n, e) as public information. One-way hash function h( ) gives unique output for different input.

User Registration phase: User U_i take his identification number ID_i to the key registration center to obtain the signature g_i for ID_i. If the center confirms the correctness and the relationship between U_i and ID_i , then center calculates g_i using:

$$g_i = ID_i^d \bmod n \qquad \text{(i)}$$

.and hands g_j to U_i as shown in figure 2. When all the users have registered and got their g_i (i = 1...n) the center does not need to exist in ad hoc network any more.

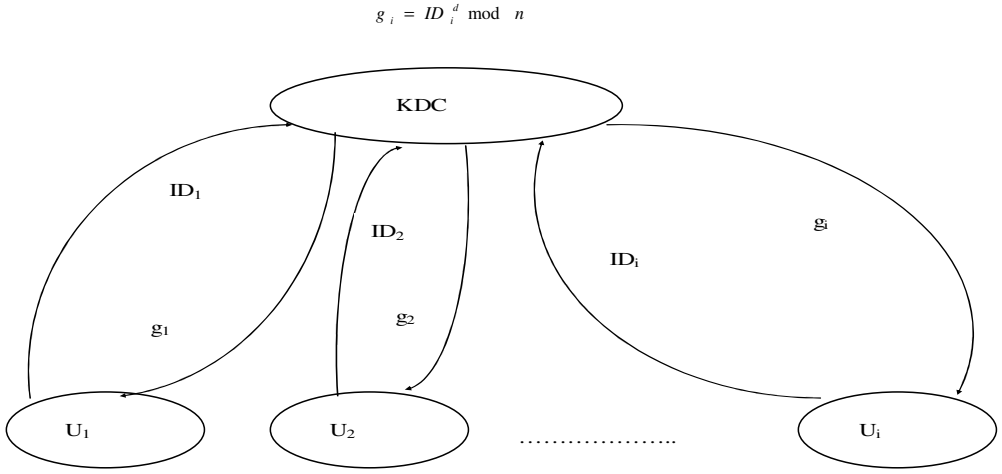


FIGURE 2: Registration phase of user with their identity

User Verification phase: Assume U_i and U_j are the two users communicate with each other. First, U_i selects a random number r_i and computes two public keys of y_i and t_i as

$$y_i = g_i.\alpha^{r_i} \bmod n \qquad \text{(ii)}$$

and

$$t_i = r_i^e \bmod n \qquad \text{(iii)}$$

Second, U_i uses a timestamp T_i and the identification number (ID_j) of user j to perform the operation of one-way function of $h(y_i,t_i,T_i,,ID_j)$, then computes

$$s_i = g_i.r_i^{h(y_i,t_i,T_i,ID_j)} \bmod n \qquad \text{(iv)}$$

Finally, U_i sends (ID_j y_i, t_i, s_i, T_j) to U_j as shown in figure 3.
Similarly, U_j selects the random number r_j and the timestamp T_j , then computes

$$y_j = g_j.\alpha^{r_j} \bmod n \qquad \text{(v)}$$

$$t_j = r_j^e \bmod n \qquad \text{(vi)}$$

$$s_j = g_j.r_j^{h(y_j,t_j,T_j,ID_i)} \bmod n \qquad \text{(vii)}$$

and sends (ID_j , y_j, t_j, s_j, T_j) to U_i as shown in figure 3.
Before generating the session key, U_i and U_j need to verify whether (ID_j, y_i ,t_i, s_i, T_j) and (ID_j , y_j, t_j, s_j, T_j) are sent from user i and user j, respectively, by checking

$$s_j^e = ID_j.t_j^{h(y_j,t_j,T_j,ID_i)} \bmod n \quad \text{(viii)}$$

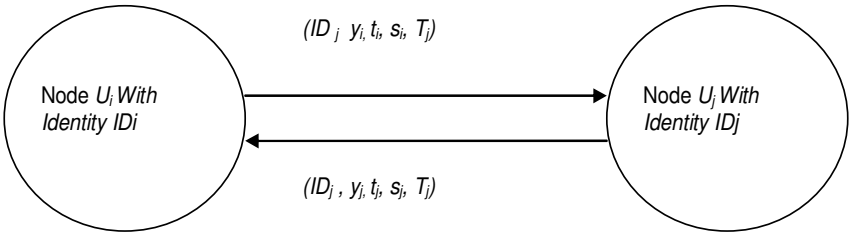


FIGURE 3: Communication between MANETs Nodes for end-to-end Authentication and Secret Shared key generation in the proposed scheme

It can be checked by user U_i as shown below:
Take L.H.S and from equation (vii)

$$s_j^e = (g_j.r_j^{h(y_j,t_j,T_j,ID_i)} \bmod n)^e$$
$$s_j^e = (g_j)^e.(r_j^{h(y_j,t_j,T_j,ID_i)} \bmod n)^e$$
$$s_j^e = (g_j)^e.(r_j^{h(y_j,t_j,T_j,ID_i)} \bmod n)^e$$
$$s_j^e = (ID_j^d \bmod n)^e.(r_j^{e*h(y_j,t_j,T_j,ID_i)} \bmod n)$$

Mathematically,
$(G^x \bmod n)^y = (G^y \bmod n)^x = G^{xy} \bmod n$
$(G^x \bmod n) \bmod n = G^x \bmod n$ because n is a very large number

$$s_j^e = (ID_j^{d*e} \bmod n).((r_j^e)^{h(y_j,t_j,T_j,ID_i)} \bmod n)$$
$$s_j^e = (ID_j^{1 \bmod \varphi(n)} \bmod n).((t_j)^{h(y_j,t_j,T_j,ID_i)} \bmod n)$$
$$s_j^e = (ID_j \bmod n).((t_j)^{h(y_j,t_j,T_j,ID_i)} \bmod n)$$

According to RSA, $d = e^{-1} \bmod \phi(n)$ and $d * e = 1 \bmod \phi(n) = 1$

$$s_j^e = ID_j.t_j^{h(y_j,t_j,T_j,ID_i)} \bmod n$$
$$s_j^e = R.H.S$$

And, similarly, user U_j verify at their end that

$$s_i^{e.?} = ID_i.t_i^{h(y_i,t_i,T_i,ID_j)} \bmod n \quad \text{(ix)}$$

Key Exchange phase: U_i and U_j compute secret session keys SK_i , SK_j , respectively, as follows: SK_i, SK_j respectively, as follows:

$$SK_i = \left(\frac{y_j^e}{ID_j}\right)^{r_j} \bmod n \quad \text{(x)}$$

$$SK_j = (\frac{y_i^e}{ID_i})^{r_j} \bmod n \quad \text{(xi)}$$

SK_i and SK_j are the same, because
Secret session can be computed by user U_i, as follows:

$$SK_i = (\frac{y^e{}_j}{ID_j})^{r_i} \bmod n$$

$$SK_i = (\frac{(g_j.\alpha^{r2} \bmod n)^e}{ID_j})^{r_i} \bmod n$$

$$SK_i = (\frac{(g_j)^e.(\alpha^{r2} \bmod n)^e}{ID_j})^{r_i} \bmod n$$

$$SK_i = (\frac{(ID_j{}^d \bmod n)^e.(\alpha^{e*r2} \bmod n)^e}{ID_j})^{r_i} \bmod n$$

$$SK_i = (\frac{(ID_j{}^{e*d} \bmod n).(\alpha^{e*r2} \bmod n)}{ID_j})^{r_i} \bmod n$$

$$SK_i = (\frac{(ID_j{}^{1 \bmod \phi(n)} \bmod n).(\alpha^{e*r2} \bmod n)}{ID_j})^{r_i} \bmod n$$

$$SK_i = (\frac{(ID_j \bmod n).(\alpha^{e*r2} \bmod n)}{ID_j})^{r_i} \bmod n$$

$$SK_i = (\frac{(ID_j).(\alpha^{e*r2} \bmod n)}{ID_j})^{r_i} \bmod n$$

$$SK_i = (\alpha^{e*r2} \bmod n)^{r1} \bmod n$$

$$SK_i = (\alpha^{e*r1*r2} \bmod n) \bmod n$$

$$SK_i = \alpha^{e*r1*r2} \bmod n$$

$$SK_i = \alpha^{e*r1*r2}$$

Thus,

$$SK_i = SK_j = \alpha^{e*r1*r2} \bmod n. \quad \text{(xii)}$$

As, n is very large generally, then

$$SK_i = SK_j = \alpha^{e*r1*r2}$$

3. ANALYSIS OF SECURITY

Several attacks are designed to analysis the security of the key exchange protocol, as the follows:

3.1 Prevention from brute-force attacks

Attack 1: The proposed scheme avoids problem of the RSA factorization. If an attacker can derive the private key d from the public key of the key generator center by computing $d = e^{-1} \bmod \phi(n)$, then he can obtain g_j by computing $g_i = ID_i^d \bmod n$; thus he can play the role of U_i to forge (ID_j y_i ,t_i, s_i, T_j) using (ii, (iii) and (iv). However derive the private key d using the operation $d = e^{-1} \bmod \phi(n)$ needs to factor the large integer n.

Attack 2: The proposed scheme avoids forgery attack.
The user U_i picks out a number R such that $ID_j = (ID_i.R^e) \bmod n$, where gcd(R,n)=l, and computes the private information of U_j using $g_j = ID_j^d = ID_i^d.R = g_i.R \bmod n$, then he can play the role of U_j to forge (ID_j,y_j,t_j,s_j,T_j). However, before picks out the number R, the security key d is required for the operation of $R = (\frac{ID_j}{ID_i})^d \bmod n$ as Attack 1, he still needs to factor n.

3.2 Prevention of replay attacks
In each of the communication sessions during key exchange, "two-way" authentication has been adopted to prevent the replaying attack. During key exchange process, user foils the replay attack by checking the freshness of datum using random number and timestamp.

3.3 Prevention of man-in-the-middle attacks
The proposed scheme avoids Man-in-the Middle attack. When U_i sending (ID_j y_i, t_i,s_i,T_j) to U_j , an adversary can intercept the datum from the public channel, then plays the role of U_i to cheat U_j or another users using (ID_j y_i, t_i, s_i, T_j) The attacker does not pass the verification of (ix) since both the timestamp T_i and the identification information ID_j are inputs of the one-way function h() and used in the operation of $s_i = g_i.r_i^{h(y_i,t_i,T_i,ID_j)} \bmod n$,

4. CONCLUSIONS & FUTURE WORKS

Key management is a fundamental, challenging issue in securing MANETs. This paper presents a secured ID-based key management scheme for MANETs which permits mobile nodes to derive their public keys directly from their known network identities and with some other common information. Most existing security mechanisms for MANETs thus far involve the heavy use of public key certificates. Our solution obviates the need of any inline Certification Authority (PKI) to share secret key. It also provides end-to-end authentication and enables mobile user to ensure the authenticity of user of peer node. The significant advantage of our solution is to avoid users to generate their own public keys and to then distribute these keys throughout the network. This scheme solved the security problem in the ad hoc network and is also suitable for application to other wired and wireless network. In this regard, we believe that the finding of this paper would have influence on the research paradigm of the whole community and stimulate many other fresh research outcomes. As our future work, we will seek efficient solutions based on our secure ID-based key management scheme to a variety of challenging security issues in MANETs such as intrusion detection and secure routing.

.

5. REFERENCES

1. David B. Johnson, David A. Maltz, Yih-Chun Hu, and Jorjeta G. Jetcheva, *"The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)*", IETF Mobile Ad Hoc Networks Working Group, Internet Draft, 15 April 2003.
2. P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum and L Viennot, "*Optimized Link State Routing Protocol for Ad Hoc Networks*", In Proceeding of IEEE Int'l MulU Topic Con!. 2001, IEEE Press, pp. 62-68, 2001.
3. Nikola Milanovic, Miroslaw Malek, Anthony Davidson and Veljko Milutinovic, "*Routing and Security in Mobile Ad Hoc Networks*", IEEE Computer. Vol. 37, No.2, pp. 61-65, February 2004.
4. L. Zhou, and Z. J. Haas, "*Securing Ad Hoc Networks*", IEEE Network Journals, Vol. 13, No.6, pp. 24-30, 1999.
5. A.Weimerskirch, and D. Westhoff, "*Identity Certified Authentication for Ad Hoc Networks*", 2003 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03), pp. 33-40, October 31, 2003.

6. menezes, P. V. Oorschot, and S. A. Vanstone, "*handbook of Applied Cryptography*", CRC Press, New York, 1997
7. B. Newman and T. Tso. , *"Kerberos: An Authentication Service for Computer Networks*", vol. 32, no. 9, pp. 33-38, Sept. 1994
8. Jiejun Kong, Petros Zerfos, Haiyun Luo, Songwu Lu and Lixia Zhang, "*Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks"*, In Proceeding of the IEEE 9th International Conference on Network Protocols (ICNP'01), IEEE Computer Society, pp. 251, 2001.
9. H. Deng, A. Mukheljee, and D.P. Agrawal, "*Threshold and Identity-based Key Management and Authentication for Wireless Ad Hoc Networks*", In Proceeding of the International Conference on Information Technology: Coding and Computing (ITCC'04), IEEE Computer Society, Vol. 1, No.1, pp. 107-111, January 2004.
10. J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "*Providing Robust and Ubiquitous Security Support for Mobile Adhoc Networks*", In Proceeding of IEEE Int'l Conf. Network Protocols, Nov. 2001
11. M. Narasimha, G. Tsudik, and J.H. Yi, "*On the Unitility of Distributed Cryptography in P2P and Manets: The Case of Membership Control*", In Proceeding of IEEE Int'l Conf. Network Protocols Nov. 2003
12. S. Yi and R. Kravets, "*Moca: Mobile Certificate Authority Wireless Ad Hoc Networks*", In Proceeding of Second Ann. PKI Research Workshop (PKI '03), Apr. 2003
13. M. Bechler, H.-J. Hof, D. Kraft, F. Pahlke, and L. Wolf, *"A Cluster-Based Security Architecture for Ad Hoc Networks*", In Proceeding IEEE INFOCOM, Mar. 2004
14. H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, "*URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks*", IEEE/ACM Trans. Networking, vol. 12, no. 6, pp. 1049-1063, Dec. 2004
15. Shamir, "*Identity-based cryptosystems and signature schemes*", in Advances in Cryptology - Crypto '84, Lecture Notes in Computer Science 196, Springer, pp. 47-53, Springer-Verlag, 1984.
16. M. Bohio, and A. Miri, *"An Authenticated Broadcasting Scheme for Wireless Ad Hoc Network*", In Proceedings of the Second Annual Conference on Communication Networks and Services Research (CNSR '04), IEEE Computer Society, pp. 6974, May 19-21, 2004.
17. A. Khalili, J. Katz, and W. Arbaugh, "*Toward Secure Key Distribution in Truly Ad Hoc Networks*", 2003 Symposium on Applications and the Internet Workshop (SAINT 2003), IEEE Computer Society, pp. 342-346, 2003.
18. H. Deng, A. Mukherjee, and D. Agrawal, "*Threshold and Identity-Based Key Management and Authentication for Wireless Ad Hoc Networks*", In Proceeding Int'l Conf. Information Technology: Coding and Computing (ITCC '04), Apr. 2004
19. N. Saxena, G. Tsudik, and J.H. Yi, *" Identity-Based Access Control for Ad Hoc Groups*", In Proceeding of International Conference of Information Security and Cryptology, Dec. 2004
20. Y. Zhang, W. Liu, W. Lou, Y. Fang, and Y. Kwon, "*AC-PKI Anonymous and Certificateless Public-Key Infrastructure for Mobile Ad Hoc Networks*", In Proceeding of IEEE Int'l Conf. Comm pp. 3515-3519, May 2005
21. A. Shamir, "*How to Share a Secret*," Comm. ACM, vol. 22, no. 11, pp. 612-613, 1979.
22. Y. Desmedt and Y. Frankel, "*Threshold Cryptosystems*", In Proceeding of CRYPTO '89, pp. 307-315, Aug. 1989.
23. R. L. Rivest, A. Shamir, and L. Adelman, "*A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*", Comm. Of ACM Vol.21, no.2, pp. 122-126, 1978.

A Trust Conscious Secure Route Data Communication in $MANET_S$

Dr. Anil Kapil anil_kdk@yahoo.com
Professor, M M Institute of Computer Technology and Business Management, M M University, Mullana, Ambala, Haryana, India

Mr. Rajneesh Gujral rgujral77@yahoo.com
Asst. Professor, Department of Computer Engineering, M M Engineering College, M M. University, Mullana, Ambala, Haryana, India

ABSTRACT

Security in mobile adhoc networks is difficult to achieve, notably because of the vulnerability of wireless links, the limited physical protection of nodes, the dynamically changing topology, the absence of a certification authority, and the lack of a centralized monitoring or management point. The major difficulty in adhoc network occurs when a new node join network but not having any trust based relation with other nodes of network. We have proposed a new mechanism that provides trust conscious secure route data communication between the Mobile nodes. In this mechanism we will dynamically increase the trust from (Low to High) between the mobile nodes using proxy node. When mobile node needs secure data communication, it will generate a dynamic secret session key with the desired destination mobile node directly or via proxy mobile nodes. These dynamic secret session keys are generated using message digest and Diffie-Hellman protocol.

Keywords: Session keys, Message digest, MANETs.

1. INTRODUCTION

$MANET_S$ are made up of collaborative mobile nodes equipped with wireless network interfaces, where each node is able to communicate with other nodes within its transmission range without any fixed infrastructure, such as a name server or switches to set up connections The security services of adhoc networks are not together different from those of other network. The goal of these services is to protect information and resources from attacks and misbehavior. These security services such as privacy, integrity and authentication cannot be achieved without a prior solid key management. The major problem in providing security service in adhoc networks is how to manage the key that provide trustworthiness and privacy in data communication. In order to design practical and efficient key management system, it is necessary to understand the characteristics of adhoc networks and why traditional key management system is not suitable to such environments. To establish a secure communication between two mobile nodes in an adhoc manner, i.e. secure peer- to -peer communication, it is necessary for the two nodes to share a secret key [1]. This can be easily achieved if we assume the existence of a public key infrastructure (PKI) [2, 3]. However, many mobile adhoc networks cannot afford to deploy public key cryptosystem due to their high computational overheads. In mobile adhoc networks, due to

unreliable wireless media, mobile node mobility and lack of infrastructure, providing secure communications is a big challenge. The symmetric key cryptography approach has computation efficiency because the algorithms are less complex and key size is small. In fact, any cryptographic means is ineffective if the key management is weak. We have proposed to implement our mechanism on reactive routing protocols, since they are more appropriate for wireless environments and they initiate a route discovery process only when data packets need to be routed [4]. Discovered source route are then cached until they go unused for a period of time, or break because of the network topology changes [5]. This paper is organized as follows the next two sections presents some of related works and overview on AODV protocol with different trust based scenarios. Section 4 gives the proposed mechanism on reactive protocol AODV.

2. RELATED WORKS

A reputation based trust management scheme for peer to peer systems has been presented in [6] [7].Here a node's trust is calculated from the reputation based on complaints lodged by its previous clients. A similar scheme with local and global reputation is discussed in [8].The distributed trust model in a general network scenario based on human approach of knowing about strangers from friends, is decentralized [9].A modified hierarchical trust Public key model, of which nodes can dynamically assume management roles, to present a framework for key that provides redundancy and robustness between pairs of nodes [10] .Similar certificate path discovery in hierarchical PKI trust model in MANET. This approach labels each CA certificate with codeword. By using the label, it designs an algorithm to speed up the process of certificate path discovery without the presence of central PKI service [11]. Another model presented for calculating Direct & Situational Trust values can be shared among neighbours using a higher layer Repudiation Exchange Protocol in [12][13]. In Gehramannet al. [14] describe a set of techniques to help two wireless devices to securely authenticates each others and agree on a shared data string via insecure wireless channel. In similar work [1], Sencun zhu et al. present a scalable and distributed protocol that enables two nodes to establish a pair-wise shared key on the fly, without requiring the use of any online key distribution center. The design of their protocol is based on a novel combination of two techniques: probabilistic key sharing and threshold secret sharing. Wen Liang Du and jing Deng [16], have also presented a new pair-wise key pre-distribution scheme for wireless sensor networks. Their scheme has a number of appealing properties. It is scalable and flexible, and nodes do not need to be deployed at the same time, that's to say they can be added after initial deployment, and still be able to establish secret keys with existing nodes. The same approach is presented in [1] for establishing a pair-wise shared key between two nodes. Each node is pre-loaded with unique key that it shares with the KDC. To communicate securely, a pair of participants obtains fresh session keys from the online server. For example, secret key protocols such as Kerberos [17] and otway-rees [18] require an interactive trusted third party, a KDC, or a key Translation center (KTC) in order to establish a shared by between any two nodes. While these schemes have been widely deployed in wired networks, this approach is not suitable for adhoc networks that are characterized by dynamic topology changes and node failures, disconnections from the network and by the fact that there is typically no online server available.

3. AODV WITH EMBEDDED SECURITY

An AODV is a reactive adhoc on demand distance vector routing protocol. In this protocol, when a node joins the network and communicates with another node, it broadcasts a route request or REQUEST packet to its neighbors. The REQUEST is propagated from neighbors to neighbors and so on, using controlled flooding. The REQUEST packet set up a reverse path to the source based on intermediate routers that forward this packet. If any intermediate node has a path already to the REQUEST destination, then this intermediate node replies with a Route Reply or REPLY packet, using the reverse path to the source. In this paper, we embedded the security requirement on AODV routing protocol using trust level. A trust level of network is defined on the bases of session keys between the nodes. Three different possible scenarios can occur. F**irst scenario,** when adhoc network is recently establishes (**Trust level equal to Low)** and a mobile

node communicates with specific destination. Source node broadcast route REQUEST and then find the shortest route with destination node either directly or through intermediate nodes using AODV protocol. Then pair-wise session keys are established between all the intermediate nodes (if any) using diffe-hellman protocol. Finally, session key will be established between source and destination nodes for secure communication. **Second scenario (trust level between Low to High):** This scenario happens when the Adhoc network is already existing but the trust is not equal to High (varies between Low to high). When a source node sends a REQUEST packet to a specific destination, the intermediate node checks that is their any long trust pairing with the generator node of the actual request using AODV protocol. In this case, the route discovered by AODV between two nodes may not be the shortest route in terms of hop-count, as shown in figure1. However, AODV was able at least to find a route with a guarantee of security and key pairing between the nodes. If all the nodes on the shortest path (in term of hop count) between two nodes can satisfy the pair- wising requirements, AODV will find route that are optimal. AODV security restrictions may force packets to follow longer, but more secure paths. **Third scenario (Trust level equal to High)** First, let's consider the case when all nodes have a shared key with all their neighbor's node in the adhoc network i.e. the trust level is equal to high. In this case, our protocol will behave exactly like any traditional on-demand adhoc routing protocol in finding the destination node when the source node starts the REQUEST. In this case, the route found will be optimal in terms of security requirements and hop count. A fundamental issue that must be addressed in this case, is that every node is sharing (N-1) keys with others nodes, where N is the number of nodes in the network. Clearly, this scheme is not suitable for large networks since the storage required per node increase linearly with the network size.

4. THE PROPOSED MECHANISM

In this paper, we used an adhoc On-Demand routing protocol (AODV) to find the secure route through trusted intermediate nodes which have a secret shared key. Hence, our modification to the traditional adhoc routing protocol changes routing algorithm. The route discovered by our mechanism between two nodes may not be the shortest route in term of hop-count, as we show in figure1. At least, in our mechanism AODV is able to find a route with guarantee of security if one or more routes that satisfy the required security attributes exist then it will find the shortest secure route. If insecure route exist between two nodes (source & destination node), then our mechanism initiates a session key which generate a secure route directly or with intermediate nodes.

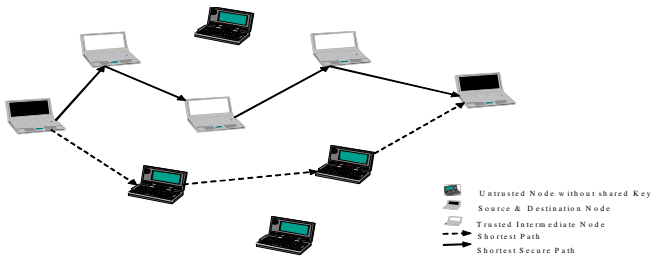


FIGURE 1: Shared key secure route in adhoc network

For establishing a long term secret between two mobile nodes first exchange their initial authentication information then establish the session key between the mobile node with Diffe-Hellman algorithm at run time. Our approach we will show two scenarios.

- Joining a new node in adhoc network and Trust relationship nil.
- A trusted Intermediate mobile node acting as a Proxy Node.

Let's imagine that the new mobile node A join the Adhoc network and wants to communicate with node that is within its range. Suppose the mobile node B is in range of mobile node A. Then the

following Packets will flow between mobile node A and mobile nodes B for secure route data communication. The proposed mechanism used some notation shown in TABLE 1.

4.1 Joining a new node in adhoc network and Trust relationship nil.

Step1: Initially mobile node A generates ticket for authentication to mobile node B .The mobile node A sends a ticket to mobile node B that contain

$A \rightarrow B : ID_{A,} h(K_A)$

.i.e. ID_A and hash of the number K_A .The K_A is generated by Diffie-Hellman Protocol at run time.

$K_A = (G^X \bmod N)$

Step2. Same way mobile node B sends ticket to mobile node A for authentication. The ticket contains

$B \rightarrow A : (ID_B, h(K_B))$

where, $K_B = (G^Y \bmod N)$

Step3. When mobile node A want secure communicate with mobile node B. Mobile node A generate ticket for mobile node B that contain

$A \rightarrow B : (ID_A, K_A, N_A)$

Then mobile node B use hashing algorithm and make the hash of K_A key i.e. $(h(K_A))$ compare both the hash if they are equal send reply ticket to mobile node A.

TABLE 1: Notation

G	Large size prime public number (public to every Adhoc networks node)
N	Large size public prime number i.e. $\frac{N-1}{2}$ is also a prime number
A , B, C	Mobile node A, mobile node B and mobile node C
ID_A	Identity of mobile node A
h (K_A)	The Hash Function of the Shared key K_A
K_{AB}	The Shared key between mobile node A and B
E_{AB}	Encryption using the shared key between mobile node A and B
N_A , N_B , N_C	Large random numbers selected by mobile nodes A, B and C respectively
$A \rightarrow B$	Message from mobile node A to mobile node B
(G, N)	Universally used Large prime numbers in adhoc network
(X, Y)	Secret large random numbers used by Mobile Nodes

Step4. Mobile node B sends reply ticket that contains plain text form ID_B , K_B and encrypted ticket $E_{AB} (ID_B , N_A , N_B , h(K_B))$.

$B \rightarrow A : \{ID_B, K_B, E_{AB}(ID_B, N_A - 1, N_B, h(K_B))\}$

Mobile node A receive K_B and calculate hash of K_B i.e. $h(K_B)$ and compare it with previous hash if match occurs it prove the authentication of mobile node B. Then mobile node A decrypt the ticket by secret shared key E_{AB} and check the random number N_{A-1}. It proves that the ticket is sent by mobile node B.

$E_{AB} = G^{XY} \bmod N = K_A^Y \bmod N = K_B^X \bmod N$

Step5. Mobile Node A send acknowledgment ticket to mobile node B that contain.
$A \rightarrow B : E_{AB}(ID_A, N_{B-1})$

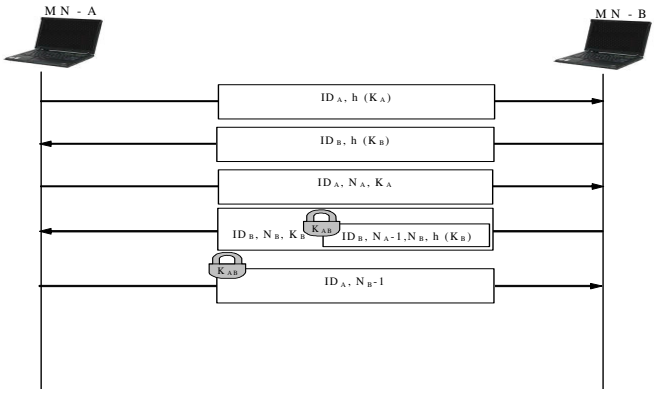
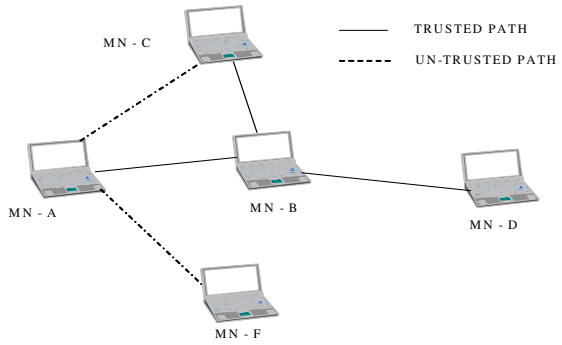


FIGURE 2: Secure Route Data Communication between Mobile Node A and Mobile Node B

4.2 A trusted Intermediate Node act as a Proxy Node

The adhoc routing protocol AODV that embedded security has presented in the section 4.1 was described only for two nodes in the same transmission range, and the procedure to establish a shared secret between them without any intermediate node. Imagine that there is nearby another mobile node C that wants to use this service. The two nodes will assist this node to establish the pair-wise keys. Let's suppose that mobile node C can communicate only with mobile node B in secure manner, and mobile node B has also a pair-wise with mobile node A. Since mobile node C shared a long term trust with mobile node B and they have a Pair-wise Key K_{BC}, mobile node B will take over to facilitate the establishment of pair-wise between mobile node C and A to Communicate with their common shared long term secret K_{AC}.We will notice through the details which will be presented in the next subsection, that mobile node B in the middle act as a proxy between mobile node A and C by forwarding the identity and the Diffie-Hellman hash of the new mobile node C to the node.



FIGHURE 3: Mobile Node B acting as Proxy Node

In this section we presented the mechanism extend the trust level of the mobile node in adhoc network in secure manner. Let's consider again the adhoc network described in figure 3. Suppose the mobile node C in the network, which for the instance contains only a trust relation with mobile node B, wishes to establish a trust relation with mobile node A .If we suppose that the mobile adhoc network contains only these three nodes, then we will increase the trust level of the network from 0 to 66 percent up to 100. We will describe in detail how to establish a trust relation in the following massages exchanged between the three nodes.

Step1: Mobile Node C broadcasts a REQUEST packet to mobile node A with its identity and its hashed Diffie-Hellman secret. When mobile node B receives this request and trusts the originator mobile node C, it forwards the identity of mobile node C and its hashed Diffie-Hellman secret to mobile node A which it trusts also.

Step2: Mobile Node A, which trusts mobile node B, will send a REPLY packet with its hashed Diffie–Hellman secret to mobile node B. This last will forward this reply from mobile node A to mobile node C. We notice that mobile node B is just acting as a proxy between mobile nodes C and mobile node A in order to establish a temporary communication channel between the two nodes.

Step3: Mobile Node C sends REQUEST Ticket with its identity $\mathrm{ID_C}$ and $\mathrm{K_C}$ to mobile node A via mobile node B.

$$\mathrm{C \rightarrow A : ID_C, K_C}$$

Step4: Mobile Node A verifies $\mathrm{K_C}$ based on $h(K_C)$. Then, it computes the shared key $\mathrm{K_{AC}}$ as a hash $\mathrm{h(G^{CA} \bmod N)}$. Mobile Node A picks a random $\mathrm{N_A}$; encrypts and authenticates $\mathrm{N_A}$, $\mathrm{h(K_A)}$ and its identity $\mathrm{ID_A}$ using $\mathrm{K_{AC}}$, and inserts the result into the REPLY packet, and finally sends the result along with $\mathrm{ID_A}$ and $\mathrm{K_A}$ to mobile node C via mobile node B.

$$\mathrm{A \rightarrow C : ID_A, K_A, E_{CA}\{ID_A, N_A, h(K_A)\}}$$

Step5: Node C receives $\mathrm{K_A}$ and computes the shared key $\mathrm{K_{AC}}$ as a hash $\mathrm{h(G^{CA} \bmod N)}$. Then, extracts $\mathrm{N_A}$ & $\mathrm{h(K_A)}$, and verifies $\mathrm{K_A}$ based on $\mathrm{h(K_A)}$, picks a random $\mathrm{N_C}$ and encrypts and authenticates $\mathrm{ID_C}$, $\mathrm{N_C}$ and $\mathrm{N_A}$ using $\mathrm{K_{AC}}$ and sends the result to node A in another REQUEST packet.

$$\mathrm{C \rightarrow A : E_{CA}(ID_A, N_C, N_A)}$$

Step6: Node A decrypt using $\mathrm{K_{AC}}$ extracts $\mathrm{N_C}$ and sends it to node C.

$$\mathrm{A \rightarrow C : N_C}$$

At this sage both C and A can calculate a shared secret key that can use to communicate securely.

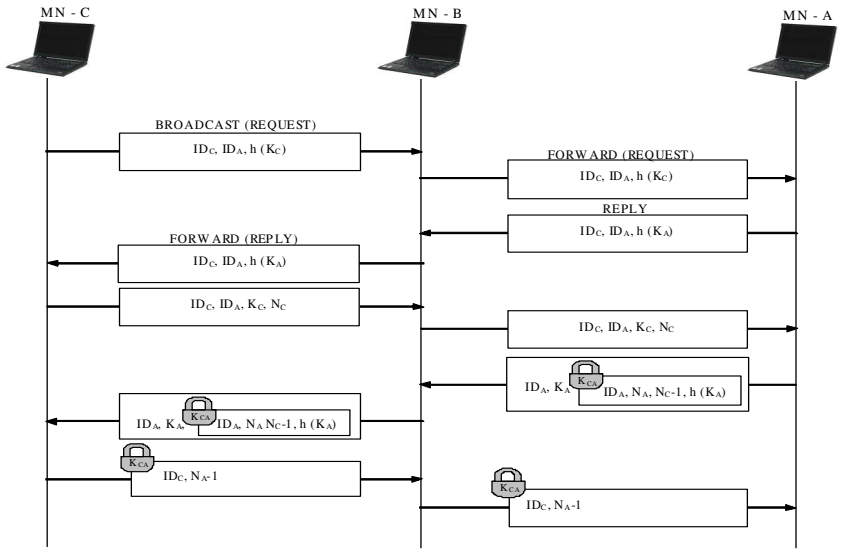


FIGURE 4: Secure Route Data communication between Mobile node C and mobile node A via Proxy mobile node B.

5. CONCLUSION & FUTURE WORKS

In most key management protocols, a trusted party is needed to act as a trust proxy node. Due to the dynamicity of adhoc networks, such central entity may easily become compromised or leave

the network. Thus, we focused in our work on proposing approach on demand protocol which enables two nodes to autonomously establish a shared key to secure further communication. Our approach is easily scalable to dynamically increasing trust directly or through proxy nodes. In future work we will add the mechanism that computes the direct Trust in a node. The accuracy & sincerity of the immediate neighboring nodes is measured by observing their contribution to the packet forwarding so that no node perform selfishness during data transfer from sender to receiver node.

6. REFERENCES

1. Sencun Zhu, Shouhuai Xu, Sanjeev Setia, Sushil jajodia , *"Establishing Pairwise Keys for Secure Communication in Adhoc Networks :A Probabilistic Ap*proach",p.p 326-331,ICNP 2003.
2. R. Housley, W. Ford, W. Polk and D. Solo, "*Internet X.509 Public Key Infrastructure Certificate and CRL Profile*." http:/www.faqs.org/rfcs/rfc2459.hunl, January 1999.
3. S. Yi and R. Kravets, "*Key Management for Heterogeneous Adhoc Wireless Networks*", IEEE ICNP'02, pp 12-15, Nov.2002.
4. C. E. Perkins and E. M. Royer," *Adhoc Networking, Adhoc On-Demand Distance Vector Routing*.",Addison-Wesley, 2000.
5. D. B. Johnson, D. A. Maltz, and 1. Broch," DSR :*The Dynamic Source Routing Protocol for Multi-Hop Wireless Adhoc Networks.",* In Adhoc Networking, ch. 5, p.p. 139-172. Addison-Wesley, 2001
6. K. Aberer and Z. Despotovic," *Managing Trust in a Peer-2-Peer Information System*.", In Proceeding of the Xth International Conference on Information and Knowledge Management, 2002.
7. K. Aberer: P-Grid, "A *self organizing access structure for P2P information system*.", In Proceeding of COOPIS, 2001.
8. B. Yu and M.P. Singh," *An Evidential Model of Distributed Reputation Management*.", In Proceeding of AAMAS 02, Bologna, Italy. Publication: ACM Press July 15-19 2002.
9. A. Abdul-Rahman and S.Hailes:" *A Distributed Trust Model In New Security Paradigma"* Workshop 1997, ACM 1997.
10. Hadjichristofi, G.C., Adams, W.J., Davis, N.J., IV, *" A framework for key management in mobile adhoc networks*", In Proceeding of the International Conference on Information Technology: Coding and Computing , IEEE Computer Society, Volume 2, pp.568-573, April 2005.
11. He Huang, Shyhtsun, Felix Wu, " *An approach to certificate path discovery in mobile adhoc networks"* , In Proceeding of the 1st ACM Workshop on Security of Adhoc and Security of adhoc and Sensor Networks, ACM, p.p.1-53,2003.
12. A.A. Pirzada,A.Datta,and C. McDonald, *" Propagating Trust in Pure Ad-hoc Networks for reliable Routing*" , In Proceeding of the International Workshop on Wireless Ad-hoc Networks (IWWAN),2004.
13 A.A. Pirzada, A.Datta, and C. McDonald, *"Trust Based Routing for Ad-hoc Wireless Networks*", In Proceeding of the IEEE International Conference on Networks (ICON'04), p.p. 326-330,2004.
14 Christian Gehrmann and Chris 1. Mitchell, "*Manual authentication for wireless devices*", Cryptobytes 2004, volume 7 No.1, 2004.
15. ENLIANG Du, JING Deng, "*A Pairwise Key Pre·Distribution Scheme for Wireless Sensor* Networks", In Proceeding of the 10th ACM conference on Computer and communications security p.p. 42-51, 2003.
16. Koh I and B. Neuman, "*The Kerberos Network Authentication Service"* (V5). RFC 1510, September 1993.
17 D. Otway, O. Rees, "*Efficient and Timely Mutual Authentication*, Operating Systems" Review, 21 (1987).

Separation of Duty and Context Constraints For Contextual Role-Based Access Control (C-RBAC)

Muhammad Nabeel Tahir m_nabeeltahir@hotmail.com
Faculty of Information Science and Technology
Multimedia University, Melaka, Malaysia

Abstract

This paper presents the separation of duty and context constraints of recently proposed Contextual Role-Based Access Control Model C-RBAC. Constraints in C-RBAC enabled the specification of a rich set of Separation of Duty (SoD) constraints over spatial purpose roles. In healthcare environment in which user roles are position and are purpose dependant, the notion of SoD is still meaningful and relevant to the concept of conflict of interest. SoD may be defined as Static Separation of Duty (SSoD) and Dynamic Separation of Duty (DSoD) depending on whether exclusive role constraints are evaluated against the user-role assignment set or against the set of roles activated in user's session. In particular, the model is capable of expressing a wider range of constraints on spatial domains, location hierarchy schemas, location hierarchy instances, spatial purposes and spatial purpose roles.
.

Keywords: Separation of duty, Constraints, C-RBAC, Location Hierarchy Schemas.

1. INTRODUCTION

Today, organizations have assumed their global presence because of advancement in intranet and internet technologies due of which organizations, today, are able to provide location based services to its customers and users anywhere, anytime. On the other hand, rapid growth in mobile technology has made it possible for the users to access organization resources, no matter, they are in static or in motion state. Because of the global presence of organizations and its widely dispersed resources and services, security of resources is the biggest threat to organization in terms of its business and even reputation. Similarly, to user and customer, the threat is the unauthorized usage of their personal and confidential information no matter by any outside intruder or employee of any company for example data entry operators, clerks, doctors, bankers etc.

In order to promise the security and correct usage of information, many countries have ratified legislation to protect privacy for individuals [1]. For example, Gramm-Leach-Bliley Act (GLB Act) [2] for financial sector, Health Insurance Portability and Accountability Act (HIPAA) [3] for medical sector in United States, Personal Information Protection and Electronic Documents Act (PIPEDA) [4, 5] in Canada have made organizations keen in knowing the user intentions in order to grant

permissions. These legislations protect and enhance the rights of consumer, clients and patients etc. while restricting access usage of the information based on the user's intentions.

In order to cope with these legislations, many access control and privacy based access control models have been proposed that have tried to ensure the security of organization resources. Some examples are time based [9, 10, 11, 12], location based [13, 14, 15, 18], Spatio temporal [16, 17] and purpose based [6, 7, 8]. However they lack in addressing an issue that how organizations can be partitioned in terms of departmental domains? Another issue that we noted is location hierarchy ambiguity.

Context Constraints

Constraints are a mechanism that help an organization lay out a higher level policy that has to be honored before every access. Constraints can apply to user-role, role-permission assignments and other factors such as time criteria to be followed before every access. An important constraint used to prevent abuse of authority is the constraint on roles to be mutually exclusive. This is related to the principle of separation of duties [18]. A similar constraint on mutually exclusive permissions also supports this principle of separation of duties for permissions. Constraints act as prerequisites on roles and permissions that any subject has to pass in order to be granted the requested role / permission. Basic event expressions used by C-RBAC constraint specification language are presented in table 1. These event expressions were used to enable/disable purposes, locations at different granularities and to define spatial purpose relationship between purpose and locations at lloc/ploc, lhs/lhi and sdom level. Through these expressions, a location can be enabled or disabled. This helps to restrict the access control decisions for a specific location or a complete set of hierarchically organized locations at location hierarchy schema/instance or domain level. These expressions also allow the administrator to enable or disable purposes or spatial purposes that are defined at a particular location or a group of locations.

Simple Event (p ∈ PURPOSE, ploc ∈ PLOC, lloc ∈ LLOC, LHS ∈ LHSS, LHI ∈ LHIS whereas ploc, lloc, LHS and LHI ∈ loc_type	
enable p or disable p	*To enable or disable purpose*
$enable_p$ *p* at *loc_type* or $disable_p$ *p* at *loc_type*	*To enable or disable purpose at different location granularities*
$assign_p$ *p* to *loc_type* or $de\text{-}assign_p$ *p* to *loc_type*	*To assign or de-assign purpose at different location granularities*
$assign_p$ *p* to *s* or $de\text{-}assign_p$ *p* to *s*	*To assign and de-assign purpose to a users' session*
enable loc_type or disable loc_type	*To enable or disable locations with different granularities like lloc, ploc, lhs, lhi or sdom*

Table 1: Events defined for purpose and location context

Table 2 shows status predicates used by C-RBAC model to check enabling/disabling, active and assignment status of purpose and location alone and also purpose with different location granularities.

Status Predicate	*Status Predicate with location and time*	*Semantics for*
enabled (p)	*enabled(p, loc_type, t)*	*p is enabled at [location loc_type] and [time t]*
enabled (p, loc_type)	*enabled (p, loc_type, t)*	*p is enabled at [location loc_type] and [time t]*
assigned (p, loc_type)	*assigned (p, loc_type, t)*	*p is assigned to [location loc_type] at [time t]*
assigned (p, s)	*assigned (p, s, loc_type, t)*	*p is assigned to users' session s at [location loc_type] and [time t]*
active (p)	*active (p, loc_type, t)*	*p is active at [location loc_type] and [time t]*
enabled (loc_type)	*enabled(loc_type, t)*	*Loc_type is enabled at [time t]*

Table 2: Status predicates for purpose and location context

Table 3 summarizes the constraint types and expressions that are applicable on purpose and location context used by C-RBAC model. For all C-RBAC constraints, time_epr define the time and loc_type define a location with different granularity:

Constraint Categories	*Constraints*	*Expression*
Purpose with location and time constraints	*Purpose enabling*	*([time_epr],[loc_type],$enable_p$ / $disable_p$ p)*
	Purpose assignment	*([time_epr],[loc_type],$assign_p$ / $de\text{-}assign_p$ p)*
Purpose with location and duration constraints	*Purpose enabling*	*([$time\_epr_1$, $time\_epr_2$],[loc_type],$enable_p$/ $disable_p$ p)*
	Purpose assignment	*([$time\_epr_1$, $time\_epr_2$],[loc_type],$assign_p$/ $de\text{-}assign_p$ p)*
location with time constraints	*Location enabling*	*([time_epr], $enable_t$ / $disable_t$ loc_type)*

Table 3: C-RBAC Constraints types

Purpose with location and time constraints These constraints were used to specify the exact time interval during which the purpose can be enabled or disabled at some location, and during which purpose over location (spatial purpose) assignment is valid. For example if the requirement is to not to authorize any surgeon in surgical ward to write patient's PHI for routine checkup between 8pm to 8am then purpose enabling constraint can be defined to disable purpose at surgical ward location with the specified time interval. Similarly if the requirement is to allow surgeon to access PHI from MinorOPT for emergency purpose then purpose assignment constraint can be defined to assign emergency purpose at MinorOPT.

Purpose with location and duration constraints These constraints are used to specify the time duration for which an enabled purpose or purpose assigned at some location is valid. These types of constraints are useful in enforcing obligation or retention policies for example if the obligation or retention policy states that no access to PHI should be granted for more than 2 hour from surgical ward for routine operation purpose then these constraints can be helpful to enforce such privacy rules to disable or de-assign routine operation purpose at surgical ward after the

specified time duration is over. Similarly if the privacy rules states that no access to PHI is granted from research department between 5pm to 8am then duration constraints with purpose assignment can be defined on research department to de-assign research purpose at the specified time.

Location with time constraints These constraints are used to specify the time duration for which a location is enabled and access decisions should be evaluated for the user requesting from that location during the specified time. These types of constraints are useful in enforcing obligation or retention policies for example if the obligation policy states that access to PHI should be granted from emergency ward between 7pm to 8am then these constraints can be helpful to enforce such privacy rules to enable emergency ward spatial domain during the specified time.

Privacy constraints on SPR enabling, activation, user-role, role-permission assignments

Table 4 shows basic event expressions used by C-RBAC constraint specification language. These event expressions are used to enable/disable spatial purposes role and to assign and de-assign spatial purpose role to users; and permissions to spatial purpose roles.

Simple Event (spr ∈ SPR, u ∈ USERS, and prms∈ PRMS	
enable spr or disable spr	*To enable or disable spatial purpose role*
$assign_u$ *spr* to *u* or $de\text{-}assign_u$ *spr* to *u*	*To assign or de-assign spatial purpose role to user*
$assign_p$ *prms* to *spr* or $de\text{-}assign_p$ *prms* to *spr*	*To assign and de-assign permissions to spatial purpose role*

Table 4: Events defined for spatial purpose role

Table 5 shows status predicates used by C-RBAC model to check enabling/disabling, active and assignment status of spatial purpose role to users; and permissions to spatial purpose role. Given a time duration and location granularity, these predicates check the status of spatial purpose role enabling and activation.

Status Predicate	***Status Predicate with location and time***	***Semantics for***
enabled (spr)	*enabled(spr, loc_type, p, t)*	*spr is enabled at loc_type at t with for p*
$assigned_u$ *(u, r)*	*assigned (u, spr, loc_type, p,t)*	*u at loc_type is assigned to spr for p at time t*
$assigned_p$ *(prms, r)*	*assigned (prms, spr, loc_type, p,t)*	*prms is assigned to spr at loc_type for p at time t*
$active_{spr}$ *(spr)*	*active (spr, loc_type, p, t)*	*spr is active at loc_type with p at t*
Can_activate(u,spr)	*Can_activate(u, spr, loc_type, p, t)*	*u at loc_type can activate spr for p at time t*
Can_acquire(u,prms)	*Can_acquire(u, prms, loc_type, p, t)*	*u at loc_type can acquire prms for p at time t*

Table 5: Status predicates for spatial purpose role

Based on the simple events and status predicates defined for spatial purpose role in table 4 and 5 respectively; table 6 summarizes the constraint types and expressions that are applicable on spatial purpose role in C-RBAC model. For all C-RBAC constraints, time_epr defines the time and loc_type defines a location with different granularity such that:

Constraint Categories	***Constraints***	***Expression***	
p ∈ PURPOSE, loc_type ∈ PLOC, LLOC, LHSS, LHIS, SDOM, u ∈ USERS, prms ∈ PRMS			
Privacy constraints on spr enabling, user-role and role-permission assignments	*SPR enabling*	*(time_epr, loc_type, p, $enable_{spr}$ / $disable_{spr}$ spr)*	
		([$time\_epr_1$, $time\_epr_2$], loc_type, p, $enable_{spr}$/ $disable_{spr}$ spr)	
	User-role assignment	*(time_epr, loc_type, p, $assign_u$ / $de\text{-}assign_u$ spr to u)*	
		([$time\_epr_1$, $time\_epr_2$], loc_type, p, $assign_u$/ $de\text{-}assign_u$ spr to u)	
	Role-permission assignment	*(time_epr, loc_type, p, $assign_p$ / $de\text{-}assign_p$ prms to spr)*	
		([$time\_epr_1$, $time\_epr_2$], loc_type, p, $assign_p$/ $de\text{-}assign_p$ prms to spr)	
Privacy Constraints on SPR Activation			
Duration Constraints	*Total active role duration*	*Per-role*	*([$time\_epr_1$, $time\_epr_2$], loc_type, p, D_{active}, $active_{spr}$ spr)*
		Per-user-role	*([$time\_epr_1$, $time\_epr_2$], loc_type, p, u, $D_{uactive}$, $active_{spr}$ spr)*
	Max. role duration per activation	*Per-role*	*([$time\_epr_1$, $time\_epr_2$], loc_type, p, D_{max}, $active_{spr}$ spr)*
		Per-user-role	*([$time\_epr_1$, $time\_epr_2$], loc_type, p, u, D_{umax}, $active_{spr}$ spr)*
Cardinality Constraints	*Total no. of activations*	*Per-role*	*([$time\_epr_1$, $time\_epr_2$], loc_type, p, N_{active}, $active_{spr}$ spr)*
		Per-user-role	*([$time\_epr_1$, $time\_epr_2$], loc_type, p, u, $N_{uactive}$, $active_{spr}$ spr)*
	Max. no of concurrent activations	*Per-role*	*([$time\_epr_1$, $time\_epr_2$], loc_type, p, N_{max}, $active_{spr}$ spr)*
		Per-user-role	*([$time\_epr_1$, $time\_epr_2$], loc_type, p, u, N_{umax}, $active_{spr}$ spr)*

Table 6: Privacy constraints on spatial purpose role for C-RBAC model

As explained earlier that a spatial purpose role can have disabled, enabled and active states. These different states lead us to define different privacy constraints of C-RBAC model shown in table 6. Specifically, these constraints can be applied to roles as well as to user-role and role-

permission assignments. Depending on the healthcare requirements, spr enabling and activation can be restricted to particular time, location and purpose.

Privacy constraints on SPR enabling This category of constraints were defined to specify the time interval, location and purpose during which spr can be enabled or disabled, and during which user-role and role-permission assignments are valid. For example, spr enabling constraints can be defined to restrict researchers to not to access medical information from laboratory for research purpose during a specific time interval. Constraints on user-role assignments can be defined to restrict users of a particular category to not to access PHI for a specific purpose, from specific location at specific time. Similarly role-permission assignment constraints restrict permission assignment to spatial purpose role during a specific time interval, from specific location for specific purposes.

Privacy constraints on SPR activation These constraints restrict users to activate spatial purpose role from the location, purpose and time duration specified in the constraint. For example total activation duration constraint on spr restricts the span of the role's activation duration in a given period to a specified value from specific location for specific purpose. After the users have utilized the specified total active duration for spr from the specified location with specified purpose, spr cannot be activated again, even though it may still be enabled. The total active duration constraint may be specified on per-role and per-user-role basis. Per-role constraint restricts the total active duration for spr. Once the sum of all the activation durations of spr reaches the maximum allowed value from the specified location and purpose, no further activation of the role is allowed and the current activations are terminated. Per-user-role constraint restricts the total active duration for spr by a particular user. Once a user utilizes the total active duration of his spr, he is not allowed to further activate spr, whereas other users may still activate it.

The maximum duration constraint per activation constraint restricts the maximum allowable duration for each activation of a spr from a specific location with specific purpose. Once such time duration expires for a user, spr activation for that user becomes invalid. However, there may still be other activations of the same spr in the system, including one by the same user in some other session from different location or with different purpose. This constraint can also be specified on per-role or per-user-role basis. A per-role constraint restricts the maximum active duration for each spr activation for any user, unless there is a per-user-role constraint specified for that user. A per-user-role constraint restricts the maximum active duration allowed for each activation of a spr by a particular user. Activation duration can be limited within a pre-specified interval.

Healthcare applications may also imply restrictions on concurrent activation of spr for controlling access to sensitive information. In order to impose such restrictions cardinality constraints on spr activations was introduced. This constraint was categorized into two types: total number of activations and maximum number of concurrent activations. With total number of activations, spr activations can be limited to N activations. This constraint can be specified as per-role and per-user-role. Per-role constraint allows at most Nactive activations of spr in a given time interval from a specific location and purpose whether these activations occur simultaneously in different sessions or at different times. Once the total number of activations equals to Nactive, users will not be able to activate spr from the specified location with the same purpose. For example, a per-role constraint can be defined on researcher role to ensure that users from research department do not access all the resources while others are denied access. Similarly, in order to restrict the number of activations for a specified user, per-user-role constraint can also be defined.

Through maximum number of concurrent activations constraint, spr is restricted to N concurrent activations in a specified time, location and purpose. This constraint on per-role based can be specified to restrict the number of concurrent activation of spr to a maximum value. For example, if only 3 doctors are on duty in emergency ward then it is easy to assume that emergency doctor role can have utmost 3 activations from emergency ward. No more than 3 activations will be allowed to perform operations. Similarly, per-user-role constraints restrict the total number of activations of spr by a particular user to a given value.

Separation of Duty (SoD) Constraints

Constraints in C-RBAC enable the specification of a rich set of Separation of Duty (SoD)constraints over roles. SoD is widely recognized to be a fundamental principle in computer security [Li et al. 2004]. These constraints are introduced to prevent conflicts of interest arising when a single individual can simultaneously perform sensitive tasks requiring the use of mutually exclusive duties. The general form of a role exclusive constraint is: ({r1, ..., rm}, n) where each r1 is a role and n and m are integers with $n \leq m$. This constraint forbids a user to be a member of n or more roles in {r1, ..., rm} [Li et al. 2004]. In a the presence of context in which the user's roles are dependent on the position and purposes, the notion of SoD is still meaningful and thus the contextual dimension is relevant for the concept of conflict of interest. This pragmatic observation has led us to define exclusive role constraints for spatial purpose roles. The work defines two types of constraints Static Separation of Duty Constraints (SSoD) and Dynamic separation of Duty Constraints (DSoD). These constraints states that a user cannot play two conflicting spatial purpose roles at enabling or activation time at given location and purposes. For example, a separation of duty constraint preventing the same user to enable the role of practitioner nurse from entering the patient PHI and head nurse for approving a patient PHI. Similarly, one should not be authorized to play the role of practitioner nurse and head nurse. On the other hand, there are also cases in which conflict arises because of spatial or purpose context. For example, an individual should not be allowed to activate the role of emergency doctor and cardiologist in emergency ward and cardiac care ward simultaneously.

A SoD relation in C-RBAC consists of a triplet: (SSoD_Name, SP_RS, n). The SoD_Name indicates the transaction or business process in which common user membership must be restricted in order to enforce a conflict of interest policy. The SP_RS is a set containing the constituent spatial purpose roles for the named SoD relation. The n designates the cardinality of the subset within the SP_RS to which common user memberships must be restricted. Cardinality greater than one indicating a combination of spatial purpose roles that would constitute a violation of the SoD policy. For example, an organization may require that no one user may be assigned to three of the four roles that represent the medical treatment function.

Static Separation of Duty (SSoD)

Preventing a user from gaining authorization for permissions associated with conflicting roles can be achieved through SSoD. SSoD allows the enforcement of constraints on the assignment of users to roles. These constraints can take on a wide variety of forms like user-based, role-based, permission-based (Jaeger, T., and Tidswell,2001). Static constraints have also been shown to be a powerful means of implementing a number of other important separation of duty policies for example Gligor et al. [1998] formally defined four other types of static separation of duty policies. The static constraints defined in this section are those that place restrictions on sets of spatial purpose roles and in particular on their ability to form UA relations. This means that if a user is assigned to one spatial purpose role, the user is prohibited from being a member of a second

spatial purpose role. For example, a static constraint preventing the same user to enable the role of Surgeon for reading the patient's PHI in surgical ward and Surgeon_MinotOPT for reading the patient's PHI from MinorOPT. Similarly the static constraint restricts the user that one should not be authorized to play the role of practitioner nurse and head nurse simultaneously at the same location for the purpose of PHI entry and PHI entry approval respectively. The formal definition of static separation of duty is given below.

Definition 1 ***(SSoD)*****:** Static separation of duty is defined as a triplet (SSoD_Name, SP_RS, n) where SSoD_Name indicates the transaction or business process in which common user membership must be restricted in order to enforce a conflict of interest policy, each SP_RS is a spatial purpose role set, and n is cardinality such that;

$$SSoD \subseteq (2SPRloc\_type\ ,\ p \times N)$$

If q a subset of roles in SP_RS, and n is a natural number ≥ 2, with the property that no user is assigned to n or more roles from the set SP_RS in each (SSoD_Name, SP_RS, n) ∈ SSoD. Formally:

$$\forall (SP\_RS,\ n) \in SSoD, \forall q \subseteq SP\_RS:\ |q| \geq n) \Rightarrow \bigcap\nolimits_{r \in t}\ AssignedUser(spr_{loc\_type,p}) = \emptyset$$

Since the SSoD property relates to membership of users in conflicting roles, the AssignedUser function shall incorporate functionality to verify and ensure that a given user assignment does not violate the constraints associated with any instance of an SSoD relation.

Consider the set SP_RoleSet = {Surgeonloc_type,p , Surgeon_MinorOPTloc_type,p}. According to SSoD definition, the constraint (SP_RS, 2) ∈ SSoD; means that an individual cannot be Surgeon and Surgeon_MinorOPT at the same time, at same location with the same purpose.

Similarly a constraint can be defined to prevent the user from playing n distinct spatial purpose roles from the same location and purposes. For example, consider a spatial purpose role <Surgeon, Loc_TypeSurgeon, PSETSurgeon>, a SSoD constraint can be defined as (SurgeonConstraint, Surgeonloc_type,p, 2) ∈ SSoD means that an individual can be a surgical doctor in at most one location depending on the loc_type and p defined for Surgeonloc_type,p.

Definition 2 (*Static Separation of Duty in the Presence of a Hierarchy*): In the presence of a spatial purpose role hierarchy, static separation of duty is redefined based on authorized users rather than assigned users as follows.

$$\forall (SP\_RS,\ n) \in SSoD, \forall q \subseteq SP\_RS:\ |q| \geq n) \Rightarrow \bigcap\nolimits_{r \in t}\ authorized\_users(spr_{loc\_type,p}) = \emptyset$$

Dynamic Separation of Duty (DSoD)

Like SSoD, dynamic separation of duty is also intended to limit the permissions that are available to the user. However DSoD relations differ from SSoD relations by the context in which these limitations are imposed. SSoD relations define and place constraints on a user's total permission space whereas DSoD constraints limits the availability of the permissions over a user's permission space by placing constraints on the spatial purpose roles that can be activated within or across a user's sessions. DSoD allow a user to be authorized for two or more spatial purpose roles that do not create a conflict of interest when acted on independently, but produce conflict of interest concerns when activated simultaneously. For example, a user may be authorized for both the roles of nurse and headnurse, where the nurse is allowed to enter patient's PHI and headnurse is allowed to acknowledge corrections in the patient's PHI. If the individual acting in the role nurse attempts to switch the role to headnurse, DSoD would require the user to drop the role nurse before assuming the role of headnurse. As long as the same user is not allowed to assume both of these roles at the same time, a conflict of interest situation will not arise.

Definition 3 (*DSoD*): Dynamic separation of duty is defined as a triplet (DSoD_Name, SP_RS, n) where DSoD_Name indicates the transaction or business process in which common user membership must be restricted in order to enforce a conflict of interest policy, each SP_RS is a spatial purpose role set, and n is cardinality such that;

$$DSoD \subseteq (2^{SPR}{}_{loc\_type\,,\,p} \times N)$$

If q a subset of roles in SP_RS, and n is a natural number ≥ 2, with the property that no user may activate n or more roles from the set SP_RS in each (DSoD_Name, SP_RS, n) ∈ DSoD. Formally:

$$\forall SP\_RS \in 2^{SPR}{}_{loc\_type\,,\,p},\ n \in N,\ (SP\_RS,\ n) \in DSoD \Rightarrow n \geq 2 \wedge |SP\_RS| \geq n,\ and$$
$$\forall s \in SESSIONS,\ \forall SP\_RS \in 2^{SPR}{}_{loc\_type\,,\,p},\ \forall role\_subset \in 2^{SPR}{}_{loc\_type\,,\,p},\ \forall n \in N,\ (SP\_RS,\ n)$$
$$\in DSoD,\ role\_subset \subseteq SP\_RS,\ role\_subset \subseteq session\ roles(s)\ ) \Rightarrow |role\_subset| < n.$$

Consider a SP_RS = $\{Surgeon_{loc\_type,p}\,,\ Surgeon\_MinorOPT_{loc\_type,p}\}$. The DSoD constraint (SP_RS, 2) means that an individual cannot activate both spatial purpose roles in the same session. In other words, a surgical doctor cannot activate the role of Surgeon in Surgical and MinorOPT wards.

Similarly the constraint $\{EmergencyDoctor_{loc\_type,p},\ 2\}$ means that the role $EmergencyDoctor$ can be active in more than one ward and thus play different roles with different permissions, however if an individual be located there and the wards share a common space, then only one of such spatial purpose roles can be enabled depending on the purpose of the user.

2. CONSLUSION & FUTURE WORK

In this paper, constraints for C-RBAC were presented that enable the specification of a rich set of Separation of Duty (SoD) constraints over spatial purpose roles. Precisely, this chapter provides the specification of the context constraints based on the privacy requirements and different states of roles as explained in the previous chapter. Then privacy constraints on SPR enabling, activation, user-role, role-permission assignments were presented. Making the constraints as a

base, the study then discussed the separation of duty including static (SSoD) and dynamic (DSoD) used by the proposed C-RBAC model.

3. REFERENCES

[1]. Tahir, M. N. (2007). Contextual Role-Based Access Control. Ubiquitous Computing and Communication Journal, 2(3), 2007

[2]. U.S. Senate Committee on Banking, Housing, and Urban Affairs (1999). Information Regarding the Gramm-Leach-Bliley Act of 1999 [GLB Act]. [Online]. Available: http://banking.senate.gov/conf [2007, October 15].

[3]. Health Insurance Portability & Accountability Act [HIPAA] (1996). [Online]. Available: http://www.hipaa.org [2007, October 15].

[4]. Personal Information Protection and Electronic Documents Act [PIPEDA] (2000). [Online]. Available: http://www.nymity.com/pipeda/ [2007, October 15].

[5]. PIPEDA: Personal Information Protection and Electronic Documents Act (2004), Department of Justice of Canada [Online]. Available: laws.justice.gc.ca/en/P-8.6/text.html [2006, December 13]

[6]. Ying, C. S. (2006). Health Insurance Portability and Accountability Act (HIPAA)-compliant Privacy Access Control Model for Web Services. Master's thesis, The Hong Kong University of Science and Technology, Hong Kong.

[7]. Sidiroglou, S., Ioannidis, S., and Keromytis, A. D. (2006). Privacy as an operating system service. In Proceedings of the Workshop on Hot Topics in Security (HOTSEC), Vancouver, CA.

[8]. Protecting the Privacy of Patients' Health Information, Available: http://www.hhs.gov/news/facts/privacy.html [2007, June 28]

[9]. Bertino, E., Bonatti, P. A. and Ferrari, E. (2001). TRBAC: A temporal role-based access control model. ACM Transactions on Information and System Security, 4(3), 191–233.

[10]. Joshi, J. B. D., Bertino, E., Latif, U. and Ghafoor, A. (2005). A Generalized Temporal Role-Based Access Control Model. IEEE Transactions on Knowledge and Data Engineering, 17(1), 4–23.

[11]. Joshi, J. B. D., Shafiq, B., Ghafoor, A. and Bertino, E. (2003). Dependencies and separation of duty constraints in GTRBAC. In Proceedings, ACM Symposium on Access Control Models and Technologies, 51–64.

[12]. Joshi, J.B.D., Bertino, E. and Ghafoor, A. (2002). Temporal Hierarchies and Inheritance Semantics for GTRBAC. In Seventh ACM Symposium on Access Control Models and Technologies (SACMAT02), Monterey, California, USA.

[13]. Mantoro, T. and Johnson, C. W. (2003). Location History in a Low-cost Context Awareness Environment. Workshop on 'Wearable, Invisible, Context-Aware, Ambient, Pervasive and Ubiquitous Computing', Australian Computer Science Communications, 21(6), Adelaide, Australia.

[14]. Ray, I. and Kumar, M. (2006). Towards a location-based mandatory access control model. Computers & Security, 25(1), 36-44.

[15]. Bertino, E., Catania, B., Damiani, M.L. and Persasca, P. (2005). GEO-RBAC: A Spatially AwareRBAC, 10th Symposium on Access Control Models and Technologies (SACMAT'05), Stockholm, Sweden, 29-37.

[16]. Suroop, C. and Joshi, J.B.D. (2005). LoT-RBAC: A Location and Time-Based RBAC Model. In Proceedings of 6th International Conference on Web Information Systems Engineering, LNCS 3806, 361-375, New York, USA.

[17]. Fu, S., Xu, C. (2005). A Coordinated Spatio-Temporal Access Control Model for Mobile Computing in Coalition Environments. In Proceedings of 19th IEEE International Conference on Parallel and Distributed Processing, 289b-289b, Denver, CA, USA.

[18]. Hansen, F., Oleshchuk, V. (2003). Spatial role-based access control model for wireless networks. In Proceedings of 58th IEEE Vehicular Technology Conference (VTC'03), 2093-2097, Orlando, Florida.

COMPUTER SCIENCE JOURNALS SDN BHD
M-3-19, PLAZA DAMAS
SRI HARTAMAS
50480, KUALA LUMPUR
MALAYSIA