Secure Access Control Protocol using Group Based Access Control scheme (GBAC)

Asmidar Abu Bakar, Roslan Ismail, Abdul Rahim Ahmad
College Of Information Technology, Universiti Tenaga Nasional, Malaysia
asmidar@uniten.edu.my

Jamalul-lail Abdul Manan
Advanced Information Security Cluster, Mimos Berhad, Malaysia
jamalul.lail@mimos.my

Jamilin Jais
Imam Muhammad Ibn Saud
Islamic University, Riyadh, Saudi Arabia

ABSTRACT: Mobile ad–hoc network is a network that can dynamically be setup on the fly by mobile nodes. Due to its unique characteristics, it is becoming an attractive choice for commercial and also military application and among the many uses, is to support information sharing among mobile nodes such as in rescue mission at the disaster area. During disaster the infrastructures are partially or fully destroyed, hence temporary network that allow communication and share of information among the rescue team is required. Mobile ad-hoc network is easy to setup and requires less infrastructure, therefore it is a suitable candidate to work in disaster area. Despite its uniqueness, this network is highly vulnerable to malicious node and also to threats. In rescue mission scenario, information needs to be shared among trusted and legal nodes only hence a mechanism to restrict an access to information in this network is extremely important. In this paper, we outline the desired security properties and derive the access control requirement and used these to construct a secure access control protocol to information in MANET. We incorporate the protocol in our proposed access control scheme; the Group based access control scheme. To visualize how it works, we use the scenario based on emergency rescue mission (ERM).

Keywords: Access control scheme, Access control protocol, Mobile Ad-hoc Networks

Received: 21 August 2009, Revised 18 September 2009, Accepted 28 September 2009

1. Introduction

Mobile ad-hoc network (MANET) as defined in [12] is a type of ad hoc network that can change locations and configure itself on the fly. This network which is made from mobile devices uses wireless connections to connect to various networks such as a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission [12]. MANET is formed spontaneously and in ad hoc manner to meet an immediate demand and goal such as a group of laptops in a conference or meeting room or connected to Internet via VANET - Vehicular Ad Hoc network (one type of MANET that allow vehicles to communicate with the roadside equipment) [12]. As MANET is easy to setup, it becomes an attractive choice for use in commercial application such as in rescue mission at disaster areas [20],[22],[23],[24],[25],[26] and [27]. At disaster areas such as flood, hurricanes, large scale accidents where infrastructure is destroyed/partially destroyed [20], the rescue teams such as army, policeman, medical officer, construction engineer etc. require a platform or some sort of network that is able to be configured fast so that they can communicate and share information in distributed and effective manner in order to make the rescue mission successful. The information sharing must be among trusted and valid entities in the network. If only this information breaks in the middle and being accessed by unauthorized party i.e. a group of terrorist it may jeopardize the rescue mission. Hence a mechanism to control /restrict access in rescue mission is indeed needed to make sure that resources are shared among legal and trusted entity. Research on access control is widely proposed for distributed and pervasive computing environment [3],[4], [6],[7],[8],[9],[13],[16],[17], [18] and [19]. As for MANET, the researchers in [15] have similar concepts as ours. However, their works focus more on authorization policies and did not discuss on security properties. The

main contribution of this paper is on constructing a protocol for access control to information in emergency situation that meet the security properties.

We propose an access control scheme which assigns devices with higher processing capabilities as Master Group (MG) that act as transient Central Authority (T_CA) which issues digital tag to identify other entities that register with it. T_CA is defined as *is CA that is only available or active for the duration of its battery life.* MG is a trusted entity and all entities trusts MG following the Public Key Infrastructure (PKI) concept. In this scheme also, MG stores documents/partial of information and any request to share these information between groups will be attain by MG. The scheme describes step by step process or protocol needed to make an access to share information in MANET securely. We use emergency rescue mission (ERM) scenario to illustrate the use of the scheme. The protocol created must meet the security properties such as data confidentiality, integrity and also non–repudiation. This paper is derived based on our previous published papers on the GBAC [1] and [2] with additional information that is obtained throughout this research work.

An example of network scenario setup at a rescue mission is shown in figure 1 below. It shows a few groups (numbered as G1, G2 and G3) that setup the temporary network at the rescue site. They establish a mobile ad hoc network (MANET) using the portable devices they carry in order to do the rescue work such as communication, coordination of team and also for resources/ data sharing. The group leader known as Master Group (MG) is selected with high processing mobile devices such as laptop, and becomes the coordinator for each group and MG also acts as gateway to the off-side rescue center that provide data, knowledge and also content. The connection between MG and off-side rescue center can use technologies such as satellite network or Universal Mobile Communication System (UMTS) or Terrestrial Trunked Radio (Tetra). MG in each group is also connected with other MG in other group using access point (if available) or relay packet between adjacent members. Members (M) in each group are communicating via wireless links with their neighbors peers and those non-neighbors are communicating via intermediate nodes that relaying the packet. All nodes maintain routing tables in order to identify path for packet forwarding. Members in each group randomly move and mix around the surrounding disaster area while MG is static at the base center for each group.

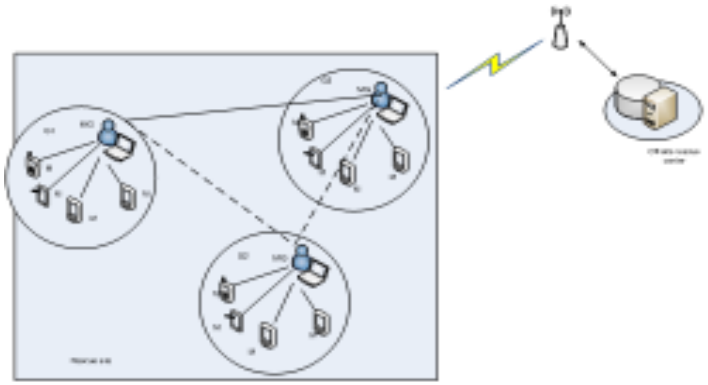

Figure 1. Example Scenario of MANET at Emergency Rescue Mission

An overview of desired security properties and an access control requirements are presented below before we describe the GBAC scheme. These two components that are important since they become the foundation in creating a secure access protocol to work in fragile MANET. The security properties are explained in section 2 while the access requirement is discussed in section 3. In section 4, the detail explanation on this model is presented. We end this paper with a conclusion in section 5.

2. Security properties

In the GBAC model, the protocol created for restricting an access to the information must meet the desired security properties. The security properties are confidentiality, integrity and non repudiation. These security properties are important to be achieved, since this will determine the either information can have secure access or not by entities in the temporary network. Below is a section on the definition on each property which is briefly explained.

i. Authenticity
This refers to the assurance that participants in communication are genuine and not impersonators [28]. In networking environment either wired or wireless it is important for the parties involved in the communication to prove their identities as what they have claimed, in order to get an access to confidential resources. With the authentic identity, user builds trust among each other. The authenticity is achieved with the use of cryptographic method such as digital signature.

ii. Authorization
Authorization is the process of granting an access to some data or resources based on user's credential. User's credential contains user's privileges and permission that is certified by the certificate authority. This credential cannot be falsified by other nodes since the information about it is stored by the certificate authority [28]. The certificate is signed by the creator and using the signature scheme with hash function, ones can verify the integrity of the certificate as well as the creator of it.

iii. Confidentiality
Confidentiality is the concealment of information or resources [29]. Another definition by E.Whitman, M., & J.Mattord, H.[30] states that the confidentiality of information is the quality or state of preventing disclosure or exposure to unauthorized individuals or systems. In this work it is defined as an access to information in ERM is given to those authorize. This is achievable with the right authentication and authorization protocol.

iv. Integrity
Bishop [29] defines integrity as the trustworthiness of data or resources while Whitman et al. [30] define integrity as the quality or state of being whole, complete and uncorrupted. We define integrity that relates with access control as making sure that the information request for sharing is not altered by any nodes in the groups except for those who have authority to do so. This can be achieved using the cryptographic hash function.

v. Non-repudiation
Non-repudiation is the assurance that someone cannot deny something. Typically, non-repudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated [31]. In this work we use the same definition as that given. Similar to authentication, the non-repudiation can be achieved using the digital signature.

Having listed all the security properties; a requirement for control the access in GBAC is needed. This access control requirements are proposed based on the desired security property and used the information security best practices as the guidance [33]. The lists of the access control requirements are discussed below:

3. Access Control requirements

i. An access to information/resources is given only to authorized nodes. The nodes authorization can be achieved via tag, identification or trust value assigned to them. In rescue environment, the situation is very chaotic; with many rescue groups and volunteers; nevertheless access to information must be restricted to authorized nodes since information may contain confidential data. With this requirement, the confidentiality properties can be achieved.

ii. Level of access right needs to be determined. In this case, not all nodes that constructed the network are given the same access right. For example, the leader in each group is given an access such as READ and WRITE. This is because the leader keeps the information that belongs to the group and he/she needs to update the information in ERM. Meanwhile the ordinary members in the group should be given READ only permission as they cannot modify the contents they received. This is important to preserve the integrity of the documents.

iii. An access to information between nodes involved needs to be restricted. This is important as not all information is sharable for all members in the rescue site. There are some information that may need to preserve its privacy and confidentiality. Example, in ERM, a man's health record is very confidential and need more privacy than information on road conditions. By determining who has access to restricted data, the confidentiality and privacy of data is well preserved. This requirement is achieved using the authentication and authorization property.

iv. Information sharing between nodes should be limited to a particular group only and not to include other groups that setup

the network or to any other random node. Example, security information should be shared among members of security group such as policeman and fireman, and general information about the rescue mission can be shared to all members in the network. This will ensure data confidentiality.

v. Delegation of authorization to other nodes is required. Since MANET is made up from groups of mobile nodes that have constraint in term of battery life therefore delegation of access permission /authorization should be disseminated to members in the same group. This is important to make sure the information needed is always available and accessible among nodes in the network particularly in ERM environment.

iv. The sharing of information must only be available during the network establishment. Once the network is dissolved, no more information sharing should occur. This requirement is important since it will preserve the confidentiality and privacy of data been shared. As MANET is developed to accomplish certain task at the specific timeframe therefore once the network is dissolved, no more sharing of information should be done.

4. Group Based Access Control (GBAC) scheme

Group Based Access Control (GBAC) scheme is constructed based on the concept of group and Role based access control (RBAC) with the use of transient CA. In this scheme, the rescue team is divided into groups based on their roles, for example, Policeman is to make sure the safety of the disaster site, while Fireman is to save people who are trapped in the buildings, Medical officer is for early treatment at the site, etc. For each group a Master Group (MG) is selected to lead the group. MG is acting as a temporary Central Authority (CA) as in normal network, but in this case it is transient. This is because MG is created using portable devices such as laptops that work based on battery (assuming no electricity is available). In this scheme, entities belonging to the same group will register with each MG and MG will issue the digital tag as entity identification and to establish trust between group members. MG also stores the shared document belonging to the group and handles the request for information sharing.

There are three phases involved in GBAC scheme, namely, prior network setup, during network setup and network dissolved. The scheme has the following assumptions in order for it to work during ERM.

- Each MG is registered with trusted root certificate (R_CA) prior to network setup and this is done off-line.
- Each MG must trust each other
- Members that are registered with each MG are trusted entities.

To simplify the writing, the following notation in table 1 is used.

Notation	Description
GP,GM,GF	GP – Group PolicemanGF – Group FiremanGM- Group Medical
M/EMG	Member /EntityMaster Group
ERM	Emergency rescue mission
OOs, Og, Om	Object- the requested information Os- information related to security, Og- information related to general info, Om- information related to medical.

Table 1. Notation and its meaning

4.2 Access Control Policy (ACP) based on concept of group and role

The access control policy for GBAC is constructed for MG in order to allow MG to restrict access to information based on level of authorization held in each member's tag. This is important since not all information is sharable within member in the same group on inter-groups. For GBAC scheme, the access policy is stated as below.

1. *For all entity in Group P, F and E and status is member, they can READ object related to security and general info.*

· $\forall E \in GP \vee GF\ GE \quad S = M, A = R\ (O = (Os\ Og))$

2. *For all entity status Master Group in Group P, F, E they can READ and WRITE object related to security and general info.*

· *E* GP GF *GE* *S = MG, A = R* W (*O = (Os Og)*)

3. *For all entity status member in Group M can READ only object related to medical and general info.*

· *E* GM *S = M, A = R* (*O =(Os Og)*)

4. *For all entity status Master Group in Group M can READ and WRITE object related to medical and general info.*

· *E* GM *S = MG,A = R W* (*O = (Os Og)*)

These policies are kept by each MG in each group. Only MG in each group has the authorization to modify the policy. This is because MG is given 'READ" and "WRITE" authority while member in the group will only be given "READ" authority. The policy is constructed based on these roles since not all members in the same group is allowed access to the same information and also not all group can access to the same information. For example, information related to medical can only be access from member from Medical group.

There are three phases in GBAC model which are prior network setup, during network establishment and network dissolve. These phases comprises of the following building blocks.

- Member registration
- Tag creation
- Protocol for access data

During the first phase is the registration of member and creating the tag for member authentication and authorization.

i. Member registration

All entity (*E)* status as Member *(M)* registers with each Master Group (*MG*). To simplify the process, the entire chapter will used *E* to represent member. The registration of *E* is conducted prior the establishment of MANET at the ERM. The registration is done off-line and upon registration, *MG* creates a tag for each *E*. The purpose of each tag is to bind the identity of E with the group. The registration needs to be done as this will allow MG to monitor members in the group. During registration also, MG stores all related information regarding members in its database such as entity name, the public key and status. This later can be used for checking members' authenticity.

4.3 The building block for GBAC model

ii. Tag creation

Tag is a token that is temporary created and is given to each registered entity during the rescue mission. It is similar to token/ ticket given to user each time user want to play or enter a place. The tag binds user identity with his public key and also group identification. The tag is created using Simple public key infrastructure (SPKI) format. This format is chosen because it provides both authentication and authorization together in one certificate. This is better than X.509 where it mainly provides for authentication. *E* uses a tag to access information in his own group as well as access betweens the same group. The tag consists of the following fields as stated in figure 5.3.2 and table 5.3.2 describes each fields.

U_ID	*G_ID*	*S*	*U_Pk*	*MG_Pk*	*A*	*T_C*	*T_E*	*Sign*

Figure 2. The tag created for each member

Symbols	Descriptions
U_ID	UserID - the identification of user/entity
G_ID	Group identification of an entity
S	The status of entity either MG =Master Group or M=member
U_Pk	Entity public key.
MG_Pk	Master Group's public key.
A	Refer to action entity obtained. If entity is MG then he can READ, DELETE, WRITE the information shared, if M then he only can READ.
T_C	T_C is the time created for the tag
T_E	T_E is the time expires for the tag.
Sign	Refer to MG signature on tag given to each registered entity.

Table 2. Symbols used in each tag and their descriptions

MG applies the cryptographic method such as digital signature scheme with cryptographic hash function to sign each tag. Using digital signature scheme with cryptographic hash function *MG* is able to authenticate the creator of the tag. This process will prove that *E* is an authorized entity from the group that setup the temporary network at the disaster area since only authorize entity is given a tag to access the information. Below, the example of signing and verifying tag using RSA signature scheme is presented. The signing and the verification process can be applied to any message. In this example, the message is the tag, denoted as *m.*

RSA signature scheme [10],[14],[5]

The signature is created using the RSA signature scheme with the assumption that the RSA security is based on the difficulty of factoring large integers.

i. System setup:
MG chooses two large secret prime numbers *p* and *q* and computes *N=p.q. MG* choose an exponent *e* that satisfies *gcd(e,(p-1)(q-1))=1. MG* public key is *(N,e)* that is publish to every node in the network or known to his peer node. *MG* calculates his public key using the extended Euclidean algorithm to *e* and *(p-1)(q-1)* and obtains the decryption exponent *d* which satisfy $e.d \equiv 1 \pmod{(p-1)(q-1)}$. This is *MG* secret key.

ii. Create and sign the tag:
MG creates a tag for each registered member (*E)* following the format in figure 5.3.2 above and signs the tag using the digital signature scheme. *MG* uses a publicly known collision resistant hash function *h:{0,1}* à {0,….,n-1)*. Using cryptographic hash function *h*, it is possible to make RSA into signature scheme without message recovery that is suitable and efficient for long messages. To sign the tag *(m)*, the following steps are performed:

1. *Compute h(m)*
2. *Apply the RSA decryption algorithm to generate the signature to h(m)using MG's secret key.*
   - $s=h(m)^d \pmod N$

In the signing process, *MG* signs the hash value of tag, *m.MG* then sends the tag *(m)* with the signature *s*, together as the pair *(m,s)*, to register *E*

iii. Verify the tag
When *E* requests to share the information from Group *X* , *E* needs to submit his tag to *MG X*. To verify the signature on the tag (*m)* , *MG X* performs the following steps:

1. *Encrypt the signature, s using RSA encryption algorithm to recover h' using MG's public key,(N,e).*
   - $h'=s^e \pmod N$

2. Compute the hash value of tag (m),h(m)

3. Check h'=h(m), if they are same, then accept the signature as valid, otherwise reject it.

In this scheme, only the hash value, *h(m)* can be reconstructed and not the whole document. This means that, the verifier can only verify the signature of *m* if he has the message, *m* given to him. The second phase in GBAC is after network has been setup at the ERM. In this phase, an access to information is permitted.

Protocol to access the information

The protocol to share the information that belongs to any group in the network at the rescue site in this research is between *E* and *MG* in the same group and also between *E* and *MG* in the different groups. The interaction is follows the concept of client-server where *MG* acts as server and *E* as a client. Intermediate nodes between *MG* and *E* will act as routers that help in forwarding the message. There are two cases that will be presented here to demonstrate the protocol. The first case is the protocol to access data between E and MG in the same group. This protocol is called Intra-access protocol. The second case is the inter-access protocol, which means the access is between *E* and *MG* from different groups in the ERM.

i. Intra-access protocol

The intra-access protocol is simulated using the scenario below.

Scenario: Entity *E* from *Group P*, known as *Ep*, request to access information regarding road safety which is confidential to other groups and also within the members of *Group P*. The interaction between *Ep* and *MG P* uses the message sequence as shown in figure 3 below. This message sequence contains registration process, tag creation and request for information using the tag created. The registration and tag creation is done offline. The process has been shown in phase 1.

Figure 3. The message sequence between MG and E in same group

When request to share information between *E* and *MG* happens as shown in sequence number 2 as in figure above, the following steps are carried out:

1. *E* submits his tag to *MG* for authentication and authorization.
2. *MG* verifies the tag
3. Based on the result obtained from the verification process, the result is either to allow or not allow.

System setup: Let assume *MG's* public key is *(N,e)* and the secret key is *d*. *Ep's* public key is Ep_{pk}, and tag is represented by the symbol *m*. The encryption and decryption is using the notation *E* and *D* respectively. Signing function is denoted by $Sig_x(m)$ which means *tag(m)* digitally signed by *x* and *h(.)* is a one way function.

Protocol :

1. E_p sends his tag, *m* and attaches with signature, *Sig* to *MG P*. *Ep* encrypts the request for sharing information using *MG P* public-key.
   - $Ep \rightarrow MG\ P : Sig_{MG\ Pd}(m)$

- *Ep* → *MG P:* $E_{MG\ P(N,e)}$*(Request(O=Os))*

2. Upon receiving the tag, *m* and request, *MG P* needs to authenticate *Ep* as an authorized member. The group identification, G_*ID*, in the tag indicates that *Ep* comes from Group P, then *MG P* uses his public key *(N,e)* to verify the signature on the tag.
   - *MG P* → *Ep : verify* ($Sig_{MG\ Pd}(m)$)
     - $h' = (Sig_{MG\ Pd}(m))^e \pmod N$
     - *MG computes the hash value of m, h(m)*
     - *If h'=h(m), the signature on m is valid.*
   - *MG P Ep: comfirm (m)*
   - *MG P* → decrypts the encrypted message using his secret key, *d*, and checks the request.
     - → *MG P Ep:Dd(Request (O=Os))*

3. *MG P* verifies request and policy in database, if request is equal to access control policy (ACP) then access is granted else access is denied.
   - *MG P* → *check database,((O=Os and GroupID=P,F,E))*

     If check database == true

     then

     Access is granted

     else

     Access is deny

4. Upon approval, E_p now can access the object requested. In ACP it is stated that member can have action READ, therefore *Ep* can only READ/VIEW the information. *MG P* creates hash value of object S to make sure the object is not altered and encrypts the object S using *Ep's* public key. *MG P* signs the object which later can be verified by *Ep* using *MG P's* public key to authenticate the sender. *Ep* downloads the object and decrypts the object using his own secret key. If the signature is valid this means that the object is sent by the right entity. *Ep* also computes the hash value of object to make sure that the contents is not altered by an attacker. The symbol || show the message concatenation.
   - *MG P:h'=h(Os)*
   - *MG P* → *Ep :* $E_{Ep\ pk}(h')||Sig_{MG\ Pd}(Os)$
   - *Ep:* $D_{Ep\ sk}(E_{Ep\ pk}(h')||\ Sig_{MG\ Pd}(Os)$
   - *Ep: verify* $(E_{Ep\ pk}(h')||\ Sig_{MG\ Pd}(Os)_{MG\ P\ (N,e)}$

Analysis of the protocol

The above protocol is analyzed to ensure it meets the desired security properties.

i. Authenticity and authorization:
The authentication of *Ep* is done by checking the signature and the digital tag that *Ep* sends to *MG P*. The *G_ID* indicates that Ep from Group P, thus *MG P* used his own public key to verify the signature attached to the tag. *Ep* is also registered with *MG P* prior to network setup, thus *MG P* can compare the information in tag with the information he stored during entity registration. Furthermore the tag has already bound the entity identity with his own public key that is kept by *MG P*. With this no other entity can masquerade *Ep*.

ii. Confidentiality:
After authenticated as valid entity from group P, then it is confirmed that *Ep* is as what it is claimed in the tag. With this the confidentiality property is achieved since the definition of confidentiality is that an access is given to authorize entity in the group, and *Ep* is now an authorized entity. Thus using the ACP, *Ep* will get the access to the information.

iii. Integrity:
Integrity of the object refers to the message *(m)* which can be document/information that is requested to be shared and also the tag that is used as node identification.

MG P is using the hash function to create the hash value of object S and also the tag. He then encrypts the message (the hash value and the object S) and sends to Ep. Once *Ep* receives this message, he can decrypt it using his secret key and get the new hash value using the original object S received from *MG P*. If the hash value sent by *MG P* and the newly calculated hash value by *Ep* matches, therefore it confirms that the received object S is not altered.

- *MG P:h=h(Os)*
- *MG P* → *Ep* : $E_{Ep\ pk}(h)||\ Sig_{MG\ Pd}(Os)$
- *Ep:* $D_{Ep\ sk}(E_{Ep\ pk}(h)||\ Sig_{MG\ Pd}(Os)$
- *Ep: h1=h(Os)*
- *If h1=h then verify Os=true*
- *Confirm object, Os is not altered in the transmission.*

iv. Non-repudiation :
Using the digital signature attached to the tag, one can confirm the sender and therefore can achieve the non-repudiation property. In this protocol, *MG P* created the tag and signed the tag using his secret key. Using the public key of *MG P*, then the signature can be verified. *MP P* must have the pair of key in order for it to sign the tag /document. This proves that only *MG P* has indeed created/signed the tag, and sent the objects/document requested by the requestor.
If $(Sig_{MG\ Pd}(m))_{MG\ P(N,e)}$ ***== Sig MG P, then it is proven that only MG P have created and signed the tag and also the object***

ii. Inter-group access in MANET
Another request to information during ERM is between members from different groups or known as inter-group. The protocol for access information/data involving members from different group is presented in the scenario below.

Scenario: Assume that an entity, *Ep* from Group *P*, needs to use some data from group *F* in order to do his work. Figure 5.3.7 below shows the message sequence between *MG P, Ep* and *MG F*. Assume that the public key of *MG F* is *pk and the secret key is sk* . Assume also the public key and secret key of *Ep* and *MG P* is same as in Intra-access protocol.

Inter-group access control protocol:

1. *Ep* request *MG F* public key from his master group, *MG P*.
   - *Ep* → *MG P :* $Sig_{MG\ Pd}(m),m$

Inter-group access control protocol:

1. *Ep* request *MG F* public key from his master group, *MG P*.
   - *Ep* → *MG P :* $Sig_{MG\ Pd}(m),m$
   - *Ep MG P:*$E_{MG\ P(N,e)}$ *(Request(MG* F_{pk}*))*

2. *MG P* checks tag, and verify the signature in the tag. The group identification *(G_ID)* in the tag indicates that *Ep* is member of *Group P*, hence *MG P* uses his public key to verify the signature attached in the tag.

   - *MG P Ep : verify* ($Sig_{MG\ Pd}(m)$)
     - $h' = (Sig_{MG\ Pd}(m))^e \pmod N$
     - *MG compute the hash value of m, h(m)*
     - *If h'=h(m), the signature on m is valid.*
   - *MG P Ep: comfirm (m)*

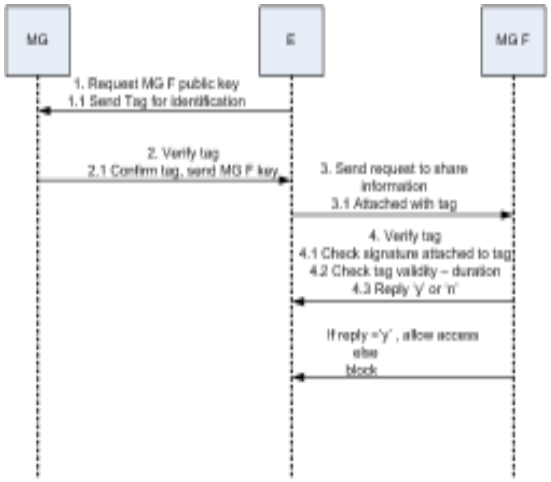

Figure 4. Message sequence between Ep, MG P and MG F

2.1 Upon confirmation of the signature in the tag, *MG P* sends *MG F* public key to *Ep*, encrypted with *Ep* public key.

- *MG P EP:* $E_{Eppk}(MG\ F_{Pk})$

3. *Ep* receives *MG F* public key, and sends request to share object, denote as *M to MG F.* Encrypt *M* using *MG F* public key. *Ep* also sends his tag to *MG F* for node authentication.

- *Ep MG F:*$(E_{MG\ Fpk}(M), Sig_{MG\ Pd}(m)$

4. Upon receiving *M*, and tag *m*, *MG F* needs to authenticate *Ep* as an entity of Group *P* as indicated in *Ep's* tag via *G_ID* field. *MG F* checks the signature on the tag using MG P public key

- *MG F :receive (M)*
- *MG F : verify* $(Sig_{MG\ Pd}(m))_{MG\ P\ (N,e)}$
  - $h'=(Sig_{MGP\ d}(m))^e (mod\ N)$
  - *MG F compute hash value of m,h(m) and compare h'=h(m)*
  - *If h'=h(m), then signature is valid and tag is authentic.*

5. In order to proceed with accessing the data, MG F needs to check tag validity. This means that MG F needs to check the *time_expires* in the tag.

If Tag submitted_ time >= time_created and <time_ expires
then check status
else
terminate

For each valid tag, it checks the information for access to the object based on the ACP stored in each MG in each group. Below, the protocol for checking the duration of tag validity is presented.

Evaluate the validity of the tag

The *submitted_time* is the time when the tag is submitted to *MG* by *E*. *Submitted_time* is not constant, it is dynamic. In each tag, there is *time_created* and *time_expires*. *Time_created* is the time when the tag is created by respective MG for the respective entity in the group. The *time_expires* is the expired time for the tag to be used.

Example, *time_created* is at 7 am, and *time_expires* is set to 24 hours, this means that if the tag is created at 7 am today, then it will be valid until 7 am the next day, in total of 24 hours. If *Ep* submits the request together with tag within the permitted 24 hours then the tag is valid. If the duration is valid, then proceed with step 5.1 else the communication is stopped.

5.1. *MG F* checks the access control policy and verifies the information in the tag.

- *MG F* → *check ACP,*
  If Ep ==(GroupID=P,F,E)and (object =Os,Og)
  then
  Access is 'yes'
  else
  Access is 'no'

6. *MG F* replies with *'y'* to *Ep*. *MG F* creates the hash value of object *S* to make sure the object is not altered and encrypts the object *S* using *Ep's* public key. He signs the message to confirm that he is the one that sends the message.

- *MG F:h'=h(Og)*
- *MG F Ep :* $E(_{Ep\ pk}(h')||Sig_{MG\ F\ sk}(Og))$

7. *Ep* downloads the object and decrypts the object using his own secret key.

- *Ep:* $D\ (_{Ep\ sk}(E_{Ep\ pk}\ (h)||\ Sig_{MG\ F\ sk}(Og)))$

Analysis on the access control protocol for inter-group

Similar to intra-access protocol, an analysis is conducted to the protocol created to ensure it meets the desired security properties.

i. Prove of authentication and authorization:
The authentication of *Ep* is done by checking the signature attached to the tag between *Ep* and *MG P* and also between *Ep* and *MG F*. The group identification indicates that *Ep* is a member of *Group P*; hence *MG P* can use his public key to verify the signature that he created. *MG F* also verifies the tag using *MG P's* public key. The signature is created with one way hash function; therefore there are no two tags that are similar. With this the signature in the tag is proven valid, and then the authentication of *Ep* is verified. Based on the status in the tag, the authorization is given to *Ep*.

ii. Confidentiality:
The confidentiality property is achieved since the access is given to authorize member only. This is based on the definition of confidentiality; an access is given to authorized entity in the network. *Ep* is an authentic member of Group *P* based on authentication module presented in (i) therefore *Ep* is allowed to get an access to security object based on ACP described in section 5.2.

iii. Integrity:

a*) Integrity of the object means that the object is not modified by the recipient.*
Ep status is member and gets an access READ to object G *(Og)*, therefore *Ep* can only READ /VIEW the object G *(Og)*.

b) The recipient can verify the object received is not altered by an attacker

MG F uses the hash function to create the hash value of *object g*. He then encrypts the message (the hash value and the *object g*) and sends to *Ep.* Once *Ep* receives this message, he decrypts it using his secret key and gets the new hash value using the original *object g* received from *MG E*. If the hash value sent by *MG E* and the newly calculated hash value is matched, therefore it is confirmed that the received *object g* is not altered. The same process is applied to verify the contents in the tag. This will ensure the content is preserved and are not altered by an attacker.

- *MG F:h'=h(Og)*
  - *MG F* → *Ep :* $E_{Ep\ pk}(h')||Sig_{\ MG\ Fsk}(Og)$
  - *Ep:* $D_{\ Ep\ sk}(E_{Ep\ pk}\ (h')||Sig_{\ MG\ Fsk}(Og)$
  - *Ep: h1=h(Og)*
  - *If h1=h' then verify Og=true*

iv. Non-repudiation:
Using the digital signature attached to the tag, one can confirm the sender and therefore can achieve the non-repudiation property. In this protocol, *MG P* created the tag and signed the tag using his own secret key. Therefore, since he is the one that has the pair of keys, then it is confirmed that only him has created the tag and sent the object.

> ***If*** $(Sig_{MG\ P\ d}(TagEp))\ Sig_{MG\ P\ (N,e)} ==$ ***Sig MG P, then it is proven that only MG P have created and signed the tag and assigned it to member from Group P.***

MG F also signs the object *O* that *Ep* request from his group. Once *Ep* receives the object, *Ep* can verify the signature using *MG F's* public key using the RSA verification algorithm above. Using the public key of *MG F*, *Ep* can authenticate *MG F* since he must have pair of key to create the signature.

> ***If*** $(Sig_{MG\ F\ sk}(O))\ Sig_{MG\ F\ pk)} ==$ ***Sig MG F, then it is proven that MG F have created and signed the object requested since he must the only one have the pair of key that created the signature.***

The last part of the phases is the network dissolution and this is happens once the rescue mission is achieved and completed. During this phase no more requests for sharing any object will be entertained by any MG. In case there is a new need for sharing of information at the site again, the whole network must be setup again and the process will need to repeat from the beginning.

5. Conclusion

In this paper, a group based access control scheme based on the concept of group and roles is presented to manage and control access to information during emergency rescue mission. The concept resembles the real emergency scenario whereby before any action is done, a briefing is conducted to various groups on how the MANET is created and what information that each groups holds and who will have control over sharing of information. A leader is chosen among group members to lead the group. There are three building blocks in this scheme which involves prior network setup, during network establishment and after network is dissolve. Prior network setup is split into two activities, namely, member registration and tag creation and an access to information is allowed during network establishment. Two access control cases have been presented to visualize the scenario in ERM and protocols for restricting an access have been constructed to make sure that access to private and confidential data meets the desired security properties such as authentication, authorization, confidentiality, integrity and non-repudiation. These properties are achieved by using the cryptographic methods such as digital signature scheme with hash function and the encryption and decryption algorithm. The proposed access control protocol was analyzed using cryptographic mechanism.

For future work, we plan to develop security protocol on delegating an access right to another entity in the network. This is important in ERM since MG in ERM is transient. Due to limited battery life, before the current MG steps down he must delegate the information and corresponding signing capabilities to a new MG. This will ensure continuous accessibility of the private information at the disaster area. The delegation of access right can be delivered using the proxy signature mechanism.

References

[1] Bakar , A.A., Ismail, R., Manan.J.A, Ahmad, A.R., Jais, J (2009). Group Based Access Control scheme(GBAC): Keeping Information Sharing Secure in Mobile Ad-Hoc Environment, *In*: Fourth International Conference on Digital Information Management(ICDIM 2009), University of Michigan, Ann Arbor, Michigan, USA, 1-4 November 2009.

[2] Bakar, A.A., Ismail, R., Manan, J.A., Ahmad, A.R., Jais, J (2009). Group Based Access Control Scheme: Proof of method for Secure Access Control Architecture in Mobile Ad-Hoc networks, *In:* The Fourth International Workshop on Broadband and Wireless Computing, Communication and Applications in conjunction with iiWAS 2009 and MoMM,2009, December 14 - 16, 2009, Kuala Lumpur, Malaysia.

[3] Corradi, A., Montanari, R., Tibaldi, D. (2004). Context-based Access Control for Ubiquitous Service Provisioning, *In*: Proc.of the 28th Annual International Computer Software and Applications Conference (COMPSAC'04), IEEE, 2004.

[4] Tanvir, Anand., Ahmad, T., Devdatta, K., Richa, K., Komal, K. (2004). Context –Based Secure Resource Access in Pervasive Computing Environments, *In:* Proc.of the second IEEE Annual Conference on Pervasive Computing and Communications

Workshops (PERCOMW'04).

[5] Stinson, D.R (2002). Cryptography: Theory and Practice, CRC Press.

[6] Zhang, G., Parashar, M (2004). Context-aware Dynamic Access Control for Pervasive Applications, *In*: Proc. Of the Communication Networks and Distributed System Modeling and Simulation Conference (CNDS 2004), San Diego CA, USA. p.219-225.

[7] Gua, Y.J., Hong, F., Zhang, Q.G., Li, R. (2005). An Access Control model for Ubiquitous Computing Applications", in Proc. Second International Conference on Mobile Technologies, Application and System.

[8] Yao, H., Hu, H., Huang, B., Li, R (2005). Dynamic Role and Context Based Access Control for Grid Applications, *In*: Proc. Of the sixth International Conference on Parallel and Distributed Computing, Application and Technology (PDCAT'05), December 05-08.

[9] Jin, J., Ahn, G. J. (2006). Role-based Access Management for Ad-Hoc Collaborative Sharing, SACMAT 06, Lake Tahoe, California, USA, ACM 2006, p. 200-209

[10] Buchmann, J.A (2001). Introduction To Cryptography, Springer-Verlag.

[11] Hoeper, K., Gong, G. (2004). Models of Authentications in Ad Hoc Networks and their Related Network Properties, International Association for Cryptologic Research, http://www.iacr.org

[12] MANET (Mobile Ad Hoc Network)- http://www.techterms.com/definition/manet. Accessed on 3-3-2009.

[13] Steffen, R., Knorr, R (2005). A Trust Based Delegation System for managing Access Control, *In*: advances in Pervasive Computing: Adjunct Proc. Pervasive.

[14] Smart, N. (2003). Cryptography: An Introduction, Mc Graw-Hill, UK.

[15] Keoh, S., Lupu, LE. (2005). An Efficient Access Control for Mobile Ad-Hoc Communities, SPC 2005, LNCS 3340, Springer-Verlag Berlin Heidelberg, 2005, p.210-224.

[16] Sadat, Emami S., Amini, M., Zokaei, S (2007). A Context-Aware Access Control Model for Pervasive Computing Environments, *International Conference on Intelligent Pervasive Computing*, IEEE .

[17] Yokoyama, S., Kamioka, E.,Yamada, S. (2006). An Anonymous Context Aware Control Architecture for Ubiquitous Services, *In*: Proc.of the 7th International Conference on Mobile Data Management(MDM'06), IEEE.

[18] Seon-Ho, P, Young-Yu, H., Tai-Myoung, C. Context-Roles Based Access Control for Context Aware Applications", LNSC 4208, p. 572-580, Springer-Verlag.

[19] Lim, T.H., Shin, S.U (2007). Intelligent Access Control Mechanism for Ubiquitous Applications, *In*: 6th IEEE/ACIS International Conference on Computer and Information Science (ICIS 2007).

[20] Plagemann, T., Anderson, J., Drugan, O.,Goebel,V., Griwodz, C.,Halvorsen, P., Munthe –Kaas, E., Sanderson, N., Skjelsvik,K.S (2005). Middleware Services for Information Sharing in Mobile Ad-Hoc Networks-Challenges and Approach, Book Chapter, p.225-236, Springer, Boston.

[21] Xianxi, H., Haiyang,W,, Zhenxiang, C., Jinjiou, L. (2006). A Context, Rule and RBAC access control in enterprise pervasive computing environment, *In*: 1st International Symposium on Pervasive Computing and Applications, p. 497-502, 3-5 August.

[22] Scalavino, E., Rusello, G., Ball, R., Gowadia, V., C.Lupu, E. (2010). An Opportunistic Authority Evaluation Scheme for Data Security in Crisis Management Scenarios, *In*: Paper presented at the ASIACCS'10, Beijing, China, April 13-16.

[23] Graaf, M. d., Berg, H. v., J.Boucherie, R., Brouwer, F., Bruin, I. d., Elfrink, H., et al (2007). Easy Wireless: Broadband ad-hoc networking for emergency services, *In*: Paper presented at the The sixth Annual Mediterranean Ad Hoc Networking Workshop, Corfu, Greece, June 12-15.

[24] Mahaputra, R. P., Abbasi, T. A., Abbasi, M. S. (2010). A Propose Architecture of MANET for Disaster Area Architecture." *International Journal of Computer Theory and Engineering*, 2 (1) 1793-8201.

[25] Aschenbruck, N., Frank, M., Martini, P., Tolle, J. (2004). Human Mobility in MANET Disaster Area Simulation-A realistic Approach, *In:* Paper presented at the Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks (LCN'04).

[26] Jang, H.-C., Lien, Y.-N., Tsai, T.-C. (2009). Rescue Information System for Earthquake Disasters Based on MANET Emergency Communication Platform, *In*: Paper presented at the IWCMC'09, Leipzig, Germany, June 21-24.

[27] Lien, Y.-N., Jang, H.-C., Tsai, T.-C. (2009). Design of P2P net: An Autonomous P2P Ad-hoc Group Communication System, *In*: Paper presented at the Tenth International Conference on Mobile Data Management: Systems, Services and Middleware.

[28] Li, W., Joshi, A.(2006). Security Issues in Mobile Ad Hoc Networks-A Surve. Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore Country.

[29] Bishop, M. (2005). Computer Security : Art and Science: Addison Wesley.

[30] Whitman, E.M., J., Mattord, H. Principles of Information Security.

[31] Thomson Course Technology. (2003). Definition on non-repudiation http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci761640,00.html Accessed on 29 -5-2010.

[32] Information security best practice-controlling access and working around disasters, http://www.businesslink/gov.uk/bdotg/action Accessed on 13-10-2010.