2012 International Conference on Information and Knowledge Management (ICIKM 2012)
IPCSIT vol.45 (2012) © (2012) IACSIT Press, Singapore

Ensuring Data Privacy and Security in MANET: Case in Emergency Rescue Mission

Asmidar Abu Bakar [1], Roslan Ismail[1] , Abdul Rahim Ahmad[1] and Jamalul-Lail Abd Manan[2]

[1] College Of Information Technology, UNITEN
[2] MIMOS Bhd

Abstract. Mobile ad hoc networks (MANETs), which can be formed by groups of portable devices, cultivate new research trend in today's computing. MANET's unique features such as scalability, fault tolerant and autonomous system allowed the network to be setup with or without any trusted authority. These features make it suitable for many applications in military, commercial as well as in emergency and rescue operations. Research on MANET as a platform for supporting emergency and rescue operations has been studied by many researchers. During emergency situations, the needs of sharing the information among the rescuers are enormously vital. However, since this network is operated based on wireless environment, it is vulnerable to threats and intruders. Information flow in MANET can be intercepted and tampered and this raised a security issues in assured that information shared between nodes in emergency situation using MANET secure. Hence, a mechanism to ensure data privacy and security during emergency rescue mission is required. This paper proposed the secure access architecture that incorporate access control model, which aims to ensure data travel between groups of rescuers secure and preserved the data integrity.

Keywords: Mobile ad-hoc network, emergency rescue mission, data , security, privacy

1. Introduction

Presently, the unpredictable growth of mobile and handheld devices such as smart phones, laptops, personal digital assistants (PDA) and tablet PCs has made fantastic changes in the world of communications. These devices are equipped with wireless connectivity such as Bluetooth and WIFI, allowing the creation of autonomous, wireless ad hoc network which is known as mobile ad hoc network (MANET). In this type of network, any node in the network may function as both a data source and a router that forward packets to other nodes. Packets from a source are typically forwarded via multiple wireless hops in order to reach its destination [1]. Since nodes in MANET are created without any fixed infrastructure, the cost of creating the network is cheaper. The formation of the network is also faster compared to a wired network [2] resulting into MANET becoming the network of choice for supporting tactical applications in military communications and operations. It is also widely used in emergency services such as search and rescue operations, disaster recovery operations, commercial and civilian applications in e-commerce, business, education, entertainment and many more [3]. Scalavino et al. [4] quoted an example of a massive car accident, which happened in Mont Blanc Tunnel in 1999, which has caused the death of 39 people. In the rescue operation many agencies gathered and formed rescue teams to handle the situation. In such an emergency incident, information that rescuers need to exchange and must be protected among various agencies include personal and medical information of the victims, information on the tunnels and sewer plants, information on affected housing areas, information on the state of accidents and details of the rescue operations itself. The data and information received from the center of operation or gathered and collected during a rescue mission must be secured and made private among the rescuers and cannot be simply broadcasted to the public. Since MANET is a wireless network, it is more vulnerable to both passive and active attacks. Therefore, a mechanism to ensure data privacy and security in MANET during emergency rescue mission is required. This paper proposed secure access architecture, which comprises components for constructing access control model that is used to restrict access between groups of rescuers towards data and information, shared during rescue operation at the emergency rescue mission. In Section 2 we give an overview of emergency rescue mission and described the proposed architecture, while in section 3 we discussed on the access control model constructed using the proposed architecture. We then conclude the paper in section 4.

2. Overview of Emergency Rescue Mission

2.1. Overview of Emergency Rescue Mission (ERM)

The Federal Emergency Management Agency (FEMA) has classified disaster into two categories; natural disaster such as earthquake, wildlife fires, flood and technological disaster such as terrorism, hazardous material or massive accidents [5]. In recent years, the world had seen huge and fatal disasters such as massive earthquake in Sichuan's province in China, the cyclone Nargis in Burma and the Atlantis hurricane Ike in Cuba [6]. In such cases, to count on fixed infrastructure to be operational after the disaster is impossible since normally the existing information and communication systems in the affected areas are destroyed or partially destroyed. Therefore, to launch a rescue operation, a temporary network communication and information infrastructure needs to be constructed at the disaster area. Rescuers need to communicate among team members and to coordinate the rescue mission. Information needs to traverse from the groups and the rescue center and vice versa in order for the rescue work to run smoothly and able to save lives. The temporary communication and information system at the disaster area requires technology that can be quickly setup with less human intervention [7]. MANET is one of the suitable mechanisms for the situation at a disaster since the deployment of the network using portable devices is easy to implement with its unique characteristics such as self organization, autonomous and very light as compared to desktop and it supports multi-hop routing. The network can also easily be setup using the existing technology embedded in laptops such as WiFi. Figure 1 shows an example of a network created at the rescue area during a disaster. In this figure, there are several groups (labeled as GP, GM and GF) that setup the MANET at the rescue area. The group concept is chosen since this is the foundation of the ad-hoc network [8].

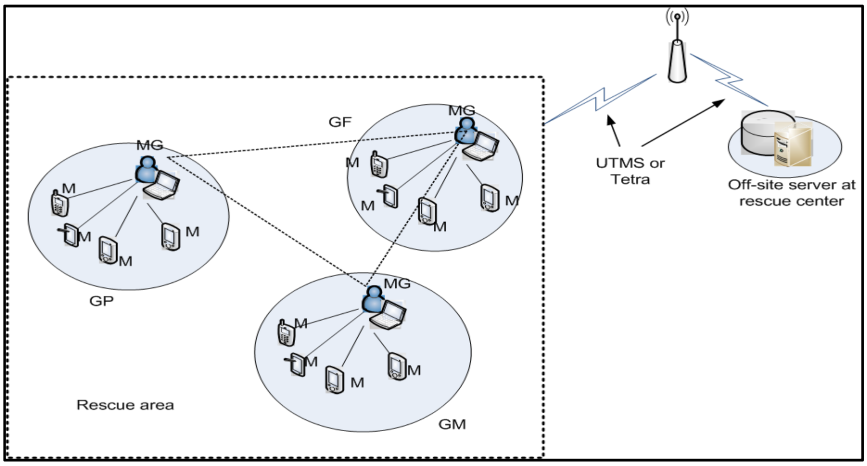

Fig. 1: MANET in Emergency Rescue Mission

There are two categories of members in each group which are normal member and leader. Members with high performance mobile devices or high processing capabilities such as laptops become the coordinator for each group. This member is known as group leader indicated as MG. MG also act as the central authority for each group as in wired network. Besides that, MG also acts as a gateway to the off-site rescue center that provides data, knowledge and also contents. The connection between MG and off-site rescue center makes use of technologies such as satellite network or Universal Mobile Telecommunication System (UMTS) or Terrestrial Trunked Radio (Tetra) [9]. MG in each group is also connected with other MGs in other groups using access points (if available) or relay packet between adjacent members. Members (M) in each group communicate via wireless links with their neighbors peers and those non-neighbors communicate via intermediate nodes that relay the packets [12]. Member use the information obtained from own MG or from other MGs in doing their work. It is assumed that all nodes maintain routing tables in order to identify path for packet forwarding. Members in each group can randomly move and mix around the surrounding disaster area while MG is static at the base center for each group. MG in each group holds the data; hence members in the group or outside the group need to send request to MG when they want to use the information. Examples of information are personal and medical information of the victims, the map of the affected area, information on the state of the catastrophe and also the information regarding the rescue operations. Data or information at the rescue area can be publicly shared among groups or accessible only by certain groups or members. MG will evaluate the member before an access is given since in wireless structure, malicious nodes may masquerade as legal nodes and get an access to confidential data or alter the data thus affecting the data integrity as well as data confidentiality.

2.2. Proposed Secure Access Architecture

Secure access control architecture identifies components and forms a suitable access control model that contains protocols for making access to information in ERM using MANET secure and able to preserved the data and information privacy. The architecture shown in Figure 2 below is designed using the client-server concept. It is in a centralized manner with every group having one active MG at a time that accepts requests from M or N. In this architecture, when member (M) sends request to share the information and acts as a client, MG a servicing node will acts as a server and a centralized authority (CA) in the group that attained the request. *i* is the symbol used to show the number of member (M) and MG involved in the interaction. Both M and MG have authentication, authorization and cryptographic protocol layers. MG has an additional layer that is used to store the group's information (indicates by resources).

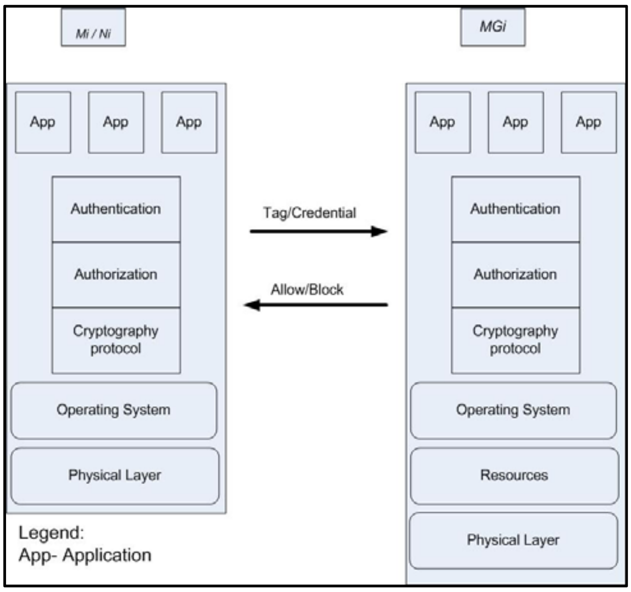

Fig 2: Client-server

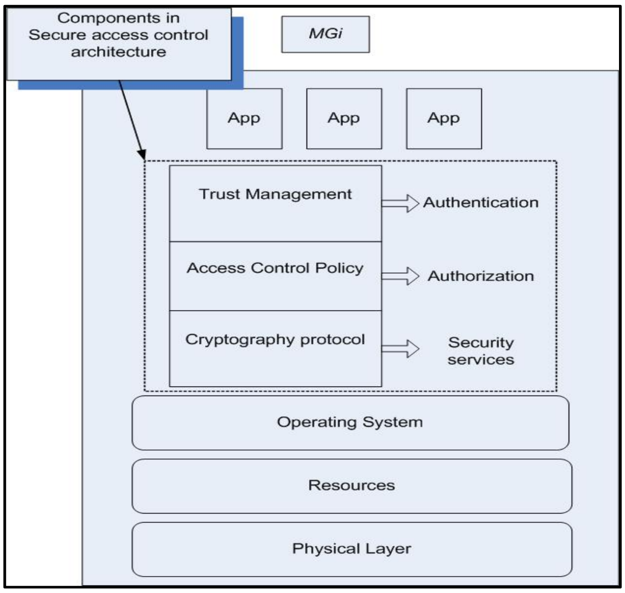

Fig 3: Component in architecture for MG

The architecture focuses on the components that reside in each MG as shown in Fig 3, which are Trust Management, Access control policy and Cryptographic scheme. The use of trust management is to authenticate users in the ERM while the Access control policy is for user's authorization on the requested object. The cryptography schemes are applied in order to ensure that data security properties such confidentiality, integrity and non–repudiation are achieved. It also used to ensure data privacy can be conserved. Using these components, the access control models that comprised of protocol for secure access is derived. Below we describe the access model which is derived from group concept.

3. Group Based Access Control model (GBAC)

The model is derived based on group and role concept, and according to [8], group can be defined as *"a set of entities that want to communicate with each other and to co-operate for some purposes"*, while Sandhu [10] defined group as *"a collection of users who have similar security attributes"*. In this research,

Group (G) consists of a set of users ***(U)*** under the same organization and a set of objects ***(O)*** related to group's function. G can be described as ***G* = *{U,O}* where *U* = *{U1,U2,……Ui}*** ∩ ***O={O1,O2,….Oi}***

An *object* represents the information that each group is holding which are related to their roles in ERM. Object can be categorized into two categories; *sensitive* or *general*. For example, in group medical, victim's health information can be classified under sensitive, while information on status of emergency situation can be classified as general since all groups involved in emergency rescue mission as well as the society needs to know this type of information. In the GBAC model, each group has objects related to their roles and object's owner is responsible for classifying the objects. A *role* in RBAC is a set of users and permission [10] . A r*ole* can also be defined as a job function within the context of an organization with some authority and responsibility given to the user [11]. In this model, the definition of role given by Memon [11] is used. Thus in GBAC model, each group has a predefined roles or tasks which was given prior to network setup at ERM and it is determined by the *group-role* relationship which is defined as the roles that each user performs based on their core task in the group. In this model also, there are two types of user which is the leader (MG) and member (M). Each type of user is assigned a role which lead to permission on object and it is determined by *user–roles* relationship and *roles-permission* relationship. ***User-roles* (UR)** determine the roles that each user performs based on their core task in the group and ***Roles-permission (RP)*** determines the permission given to member towards object based on member's role. With these definitions, the relationship between user-roles (*UR)* and roles-permission (*RP)* in each group (*G)* is defined as: *Given* ***G = {U, O},*** *then* ***UR →P, RP →O,*** *therefore* ***U →P→ O*** *based on* ***UR*** *in the group.* Figure 4 show the GBAC model constructed using the *group* and *role* concepts. In this figure, it shows that group is created by *group-role relationship.* Every group has a predefined function based on group-role definition. Each group has users, and a user is associated with user-type which is determined by a *user-roles relationship.* Group stores objects related to *group-role* functions. The access control policy is also derived based on *group-role* and *user-role relationship.*

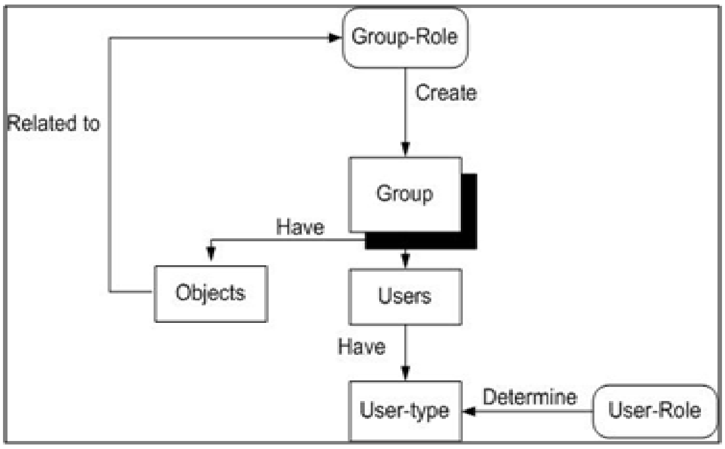

Figure 4: GBAC model construction based on group and role concepts

This model is designed to work with structured users (SU), which refers to groups, which already exist prior to disaster such as groups of army, policemen, firemen and also paramedics. They are distinguished based on a group-role relationship. The access control policy (ACP) in the GBAC model is derived based on *group-role* and *user–role* relationship and trust in this is using the concept of hierarchical public key infrastructure (HPKI). Prior to network setup at ERM, member in each group will registered with own MG and obtained a tag. Tag is a token similar to the ticket given to a user or person to play at the theme park or enter a cinema. The tag binds user with his public key, group and what user is authorized to do. This concept is similar to Simple Public key infrastructure (SPKI) certificate [13] since a user's identity is binded to his authorization. The interaction between MG and M starts when member M sends the request for data information to be shared and the tag to MG. MG verifies tag and confirms member's password matches with the one stored in the database. If all these are verified then access is given based on the authorization policy embedded in the tag. The tag verification and password confirmation is equipped with the cryptographic protocols such as encryption/decryption, hash function and digital signature. The flow of data requested between MG and M also is bind with the cryptographic protocols. These processes ensure data are securely transferred between these two entities. The data privacy is achieved via cryptographic protocols also whereby only authenticate and authorize member will obtained the requested data.

4. Conclusion

The proposed architecture consists of trust management, access control policy and cryptology protocols. With the proposed architecture, a comprehensive access control model is constructed to support the access to data and information required during emergency rescue mission. Using the access control model, members will be verified using the cryptographic protocols such as encryption/decryption, hash function and digital signature. This will ensure that only authenticated member, belong to correct group get an access to the information requested. The used of tag which was created prior to network setup at the ERM, enabled members to be authenticated hence create trust between MG and M. Beside this, the access policy embedded in the tag also able to distinguish the role between members' of the group at the emergency rescue mission. This will eliminate wrongly data passing between members in the group at the ERM, hence ensuring data security and privacy is preserved between groups at ERM.

5. Acknowledgements

Thank you to all the reviewers for reviewing this paper.

6. References

[1] Yang, H., Ricciato, F., Lu, S., & Zhang, L. (2006). *Securing A Wireless World.* Paper presented at the Proceedings of the IEEE.

[2] Balakrishnan, V., & Varadharajan, V. (2005). *Designing secure Wireless Mobile Ad Hoc Networks.* Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA'05).

[3] Hoebeke, J., Moerman, I., Dhoedt, B., & Demeester, P. (2004). *An Overview of Mobile Ad Hoc Networks: Applications and Challenges.* Journal of the Communications Network, 3(3), pp. 60-64.

[4] Scalavino, E., Rusello, G., Ball, R., Gowadia, V., & C.Lupu, E. (2010). *An Opportunistic Authority Evaluation Scheme for Data Security in Crisis Management Scenarions.* Paper presented at the ASIACCS'10, Beijing, China.

[5] Hristidis, V., Chen, S.-C., Li, T., Luis, S., & Deng, Y. (2010). *Survey of Data Management and Analysis in Disaster Situations.* Journal of Systems and Software 83(10), 1701-1714.

[6] Tornqvist, E., Sigholm, J., & Nadjm-Tehrani, S. (2009). *Hastily formed networks for disaster response: Technical Heterogeneity and Virtual Pockets of Local Order.* Proceedings of the 6th International ISCRAM Conference, Gothenburg, Sweden.

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

[8] Maki, S., Aura, T., & Hietalahti, M. (2000). *Robust Membership Management for Ad-Hoc Groups.* Proceeding 5th Nordic Workshop on Secure IT Systems (NORDSEC 2000), Reykjavik, Iceland.

[9] Kanchanasut, K., Tunpan, A., Awal, M. A., Das, D. K., Wongsaardsakul, T., & Tsuchimoto, Y. (2007). *A Multimedia Communication System for Collaborative Emergency Response Operation in Disaster-affected Areas*. International Journal of Emergency Management 4(4), pp. 670-681.

[10] Sandhu, R. S., J.Coyne, E., Feinstein, H. L., & Youman, C. E. (1996). *Role-Based Access Control Models.* IEEE Computer, 29(2), 38-47.

[11] Memon A.Q.,(2009). *Implementing Role Based Access in HealthCare Ad Hoc networks.* Journal of Networks, Vol 4. No 3, pp. 192-199.

[12] Catarci, T., Leoni, M. d., Marrella, A., Mecella, M., Salvatore, B., Vetere, G., et al. (2008). *Pervasive Software Enviornments for Supporting Disaster Responses*. IEEE Internet Computing.

[13] Smart, N. (2003). Cryptography: An Introduction: McGraw-Hill Publication.