Clustering Oriented Architectures in Medical Sensor Environments

Eleni Klaoudatou, Elisavet Konstantinou, Georgios Kambourakis, Stefanos Gritzalis
Laboratory of Information and Communication Systems Security, Department of Information and Communication Systems Engineering, University of the Aegean, Karlovassi, GR-83200 Samos, Greece
{eklad, ekonstantinou, gkamb, sgritz}@aegean.gr

Abstract

Wireless sensor networks are expected to make a significant contribution in the healthcare sector by enabling continuous patient monitoring. Since medical services and the associated to them information are considered particularly sensitive, the employment of wireless sensors in medical environments poses many security issues and challenges. However, security services and the underlying key management mechanisms cannot be seen separately from the efficiency and scalability requirements. Network clustering used in both routing and group key management mechanisms can improve the efficiency and scalability and therefore can also be envisioned in medical environments. This paper introduces a general framework for cluster-based wireless sensor medical environments on the top of which efficient security mechanisms can rely. We describe two different scenarios for infrastructure and infrastructure-less application environments, covering this way a wide area of medical applications (in-hospital and medical emergencies). We also examine the existing group-key management schemes for cluster-based wireless networks and discuss which protocols fit best for each proposed scenario.

I. INTRODUCTION

Wireless Sensor Networks (WSN) are expected to make a significant contribution in the healthcare sector, by enabling continuous patient monitoring. This improves the quality of medical care provided, and facilitates patients' every day living by allowing them to move and carry out their normal day activities while their vital sign data are continuously being monitored by stationary or mobile health care givers.

WSN can be deployed in various medical realms such as inside hospitals for monitoring patients, hospital staff and doctors, home monitoring and long-term assistive living to help, e.g. elderly or disabled people throughout their every day activities. Sensor driven monitoring may be proved extremely valuable in medical emergencies, where an on-demand medical unit is formed, in an ad hoc manner near the location where an incident has occurred, say an accident, physical disaster etc, in order to provide primary medical aid and treatment to the victims. In this case wireless sensors can be used to monitor patients' physical condition and transfer in real time vital sign data to the corresponding hospital, emergency center or directly to individual doctors.

In general, every informative system deployed in medical premises must comply with the following well known security requirements: confidentiality, integrity, availability, authentication, privacy, non-repudiation, authorization and accountability. A great emphasis though is placed in preventing cases that can put patients' life in danger, like altering monitored information or causing a Denial of Service (DoS). Therefore, authenticity, confidentiality and integrity of sensitive medical information as well as availability of medical applications need to be ensured. Privacy is also of paramount importance, ensuring that medical information is available only to authorised users.

Given that medical services and the associated to them information are considered particularly sensitive, the employment of wireless sensors in medical environments poses many security issues and challenges. By nature, WSN are vulnerable to a number of threats identified in [1] and [2]. This is mainly due to the openness of the wireless medium, the anonymous (semi)uncontrolled terrain between various endpoints from the one hand, and native sensors' limitations to processing power and energy reserves that prevent them from employing strong cryptographic methods from the other. Moreover, in contrast to traditional WSN which employ stationary nodes, base stations (i.e. some sort of infrastructure) and transmit data at relatively low data rates, health

0-7695-3102-4/08 $25.00 © 2008 IEEE
DOI 10.1109/ARES.2008.145

monitoring requires higher data rates, reliable communication and multiple mobile receivers. For instance, Personal Digital Assistance (PDA) devices carried by caregivers.

In order to deal with the increased security requirements of medical environments, authentication and encryption are necessary. However, this implies that effective key management mechanisms must be employed. Additionally, efficient ways that those keys are distributed and managed between the sensor nodes should be established. Bearing in mind that in medical environments and WSN in general, a number of intermediate nodes participate in the data path, a group key management scheme is usually needed for secure routing and packet forwarding.

The main issue here is that existing key management mechanisms designed for fixed networks are not suitable for the constrained capabilities of wireless sensors. This is obvious when considering the nature of such environments, i.e. nodes mobility, frequent topology changes and scalability needs. Therefore, when dealing with WSN more efficient mechanisms in terms or energy resources management and scalability need to be examined.

Currently, one of the proposed architectures for efficient resource management of wireless networks is clustering. Clustering is ideal for large-scale environments and time-critical applications compared to the multi-hop model and can be particularly efficient in one-to-many, many-to-one, one-to-any and one-to-all fashioned communication. The use of cluster-based approaches optimizes network bandwidth and service discovery while addressing the needs for scalability at the same time. Moreover, several cluster-based group key management mechanisms have been proposed so far ([3], [4]) and they are considered to be more efficient from similar but traditional schemes.

In this context, many modern applications for medical environments assume that the underlying sensors network is cluster-based but they do not specifically focus: (a) on how clustering is applied to those medical realms and (b) how key management mechanisms can fit and be particularly effective on top of the clustered network.

In this paper we study how the cluster-based approach can be profitably utilized in medical sensor environments in order to deal with the aforementioned security requirements and limitations. More specifically, we propose two different scenarios based on whether the medical environment is infrastructure or infrastructure-less. This distinction fully covers the varying needs of both in-hospital environments and environments formed ad hoc for medical emergencies. After that, we examine the existing group-key management schemes for cluster-based networks and discuss which protocols adapt best for each one of the proposed scenarios. Our analysis particularly focuses on cluster-based medical deployments.

The rest of this paper is organized in 4 sections, as follows: next section presents the currently proposed cluster-based approaches for WSN and ad hoc networks and identifies previous work for the case of medical environments. In Section III we describe two different cluster-based scenarios for medical domains. Section IV examines the existing group-key management schemes for cluster-based networks. Section V concludes the paper and gives pointers to future work.

II. CURRENTLY PROPOSED CLUSTERING MECHANISMS

Clustering in wireless sensor networks was originally introduced by [5]. In this work, a hierarchical cluster-based protocol was proposed as a more efficient method in terms of energy consumption. A cluster-based WSN is divided into smaller groups called clusters. A node is chosen within each cluster to be the cluster-head, also known with the terms master or leader, and relay data to the actual gateway. Cluster-heads collect data from cluster-members and usually perform aggregation and smart filtering functions before forwarding them to the gateway or to other cluster-heads. Nodes within a cluster group do not communicate directly with the gateway or the sink node, as in flat networks, but use cluster-heads to relay data towards the gateway. Clusters may be formed in a hierarchical or multi-hop way and may be overlapping or not. A special form of clusters called a clique is formed when all nodes within the same cluster are at one-hop distance from each other.

Clusters are classified into homogeneous and heterogeneous based on whether all nodes have similar capabilities or not. This means that cluster-heads may be either nodes with similar capabilities with the cluster members, or more powerful and less energy constrained nodes. The first case requires that cluster-heads change periodically, according to various criteria and algorithms in order to avoid partial energy exhaustion of the network. In the latter case we can assume that cluster-heads in the network remain stable and can perform more energy consuming functions.

Clustering has been used in medical environments in various applications and for many purposes. For example in [6] clusters are created based on an infrastructure that uses the base station to elect the leaders of the clusters. In [7] clusters are formed ad hoc to accommodate emergency situations. In [8] the authors have applied their location-aware group membership middleware in an e-care scenario where cluster heads are responsible to send user information to the new groups the user joins while he is on the move. In medical environments, location awareness can help in tracking the nearest specialist to the

location of the patient. In [9] a 3G telemedicine application is proposed based on energy-efficiency mechanisms in large-scale and a multi-class admission mechanism. They use super-sensors as cluster-heads to query sensors for medical data and perform data aggregation, filtering and compression and forward them towards the medical center. Clustering is based on the Zone Routing Protocol (ZRP).

For security purposes [10] assumes that every patient forms a different cluster and the cluster coordinator is a special entity called PSP (Patient Security Processor) that not only relays data to the gateway but is also responsible for the distribution of the symmetric key needed for encryption. Moreover, [11] and [12] describe two mechanisms for cluster-based key management for medical applications. The first one proposes a re-keying mechanism for tree-based networks while the latter proposes a cluster-based group key management mechanism for wireless networks. They apply this mechanism in a medical environment and use a bottom-up approach to specify and distribute group keys.

Our approach differs from the aforementioned previous works in that it introduces a general framework (not case-oriented) for cluster-based medical environments on top of which security mechanisms can rely. Designing a general framework that has already provisioned the requirements and constraints of the application environment is essential because the mechanisms that will be built on top of this framework can explore the benefits of efficiency, scalability and performance.

III. OUR PROPOSAL FOR CLUSTERING ON MEDICAL ENVIRONMENTS

In order to examine how clustering architectures can be employed in medical domain, first we need to focus on a specific medical environment, since it is obvious that different deployment scenarios may have different requirements. For example, in-hospital premises usually dispose of some fixed gateways which provide access to a wired infrastructure. On the contrary, in medical emergencies usually sensors are deployed in an ad hoc manner and therefore are usually considered to be mainly infrastructure-less. As a result, in the following we propose two different scenarios, based on whether the medical environment is infrastructure or infrastructure-less.

For the first scenario we consider a hierarchical network with cluster-heads. This scenario is more suitable for environments where we can have some more powerful nodes which can play the role of cluster-heads. Consequently, we consider that cluster-heads are fixed and energy consumption is not an issue for them. If a cluster-head goes out of service another node can replace it for the specific cluster or a reorganization of the clusters can be triggered, into clusters affording bigger signal radius. For these reasons, this scenario is more suitable for in-hospital environments where we can assume or implement a basic infrastructure, that is a wired network backbone and some fixed powerful gateways, placed throughout the hospital area in order to provide full coverage for wireless access.

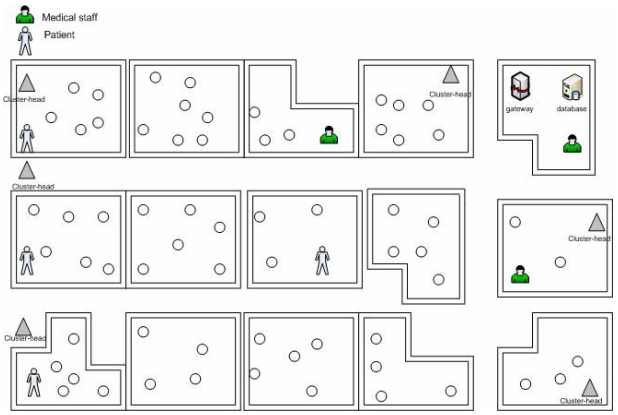

Fig. 1. Cluster-based architecture for scenario I

We can then logically break the hospital sensor network into clusters, based on their geographical location, having for example one cluster per one or more neighboring rooms and one or more clusters for the external area of the hospital. By following this grouping helps us avoid frequent topology changes each time a patient roams within the boundaries of her cluster. If the patient is transferred to another area, for example in different building or floor, she will sign out of her cluster and automatically join another one. The proposed architecture for this scenario is presented in Figure 1. Clusters' number and size may vary according to the size of the hospital, the different units and the number of sensors as well as the number of fixed-nodes or cluster-heads available and their level of wireless coverage.

Cluster members communicate with their cluster-heads every time they need to transfer data. Communication between each node and the cluster-head is typically one-hop. The cluster-head will collect those data from all nodes and forward them towards the central database. Additionally, the cluster-head can perform aggregation of the collected data or might also filter data and forward them to the central database only if the values are out of certain predefined limits (i.e. normal values). This method eliminates even more the amount of data in transit improving resource usage too. Figure 2 depicts the architecture of such a scenario and how the data is relayed to the gateway.

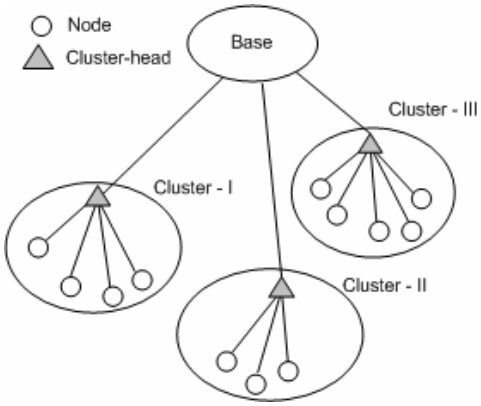

Fig. 2. Cluster organization for scenario I

For the second scenario we assume that there aren't any powerful nodes to be the cluster-heads. In this scenario, sensors can be dynamically grouped into clusters. Clusters can be overlapping or not. Every time a node has some information to transmit the node closer to the gateway (best path) is selected as the leader. The leader can either forward data straight to the gateway if it is located nearby, or forward the data via the leaders of adjacent clusters located near the gateway. To do so the leader must implement a multi-hop routing scheme like the one proposed in [13]. Communication between each node and the leader might also be multi-hop. The proposed architecture for this scenario is presented in Figure 3.

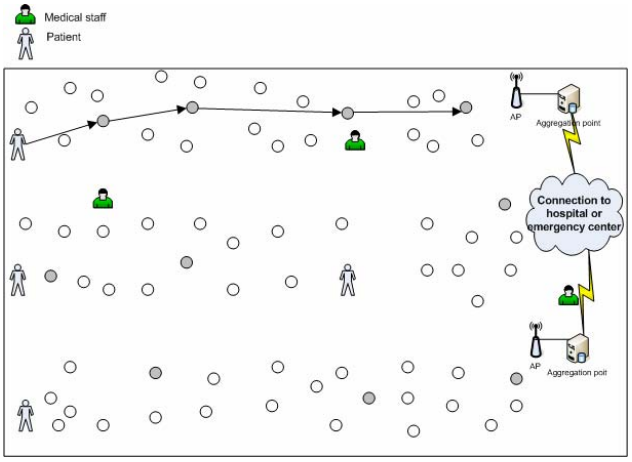

Fig. 3. Cluster-based architecture for scenario II

Having in mind that the sensors' location may change very often, the leader responsibility will be automatically assigned to the node that is located closest to the gateway or to the leaders of neighboring clusters located near the gateway. Figures 4 and 5 illustrate the way data is transferred to the gateway and an indicative topology for this scenario for the case of overlapping and non-overlapping clusters. This architecture is more suitable for medical environments where there is no full coverage or no fixed infrastructure at all, as is the case of medical emergencies.

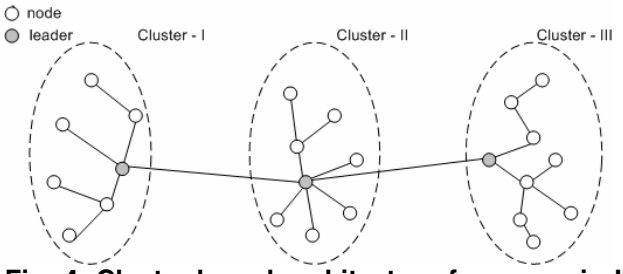

Fig. 4. Cluster-based architecture for scenario II (non-overlapping clusters)

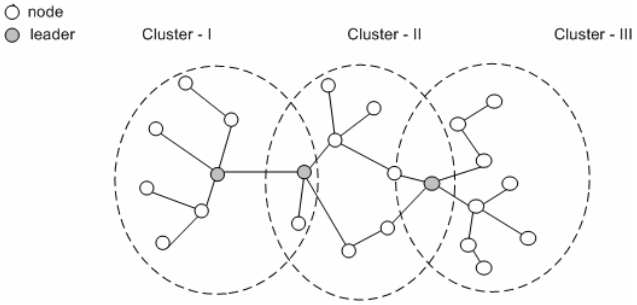

Fig. 5. Cluster-based architecture for scenario II (overlapping clusters)

The two aforementioned scenarios both take advantage of cluster-based approaches but do have significant differences. The first solution assumes an existing infrastructure, e.g. a number of fixed APs that provide full wireless coverage of the hospital area or some more powerful nodes that remain stable and might also have continuous power supply, or simply be less energy constrained. On the other hand the sensors used in this scenario can be unsophisticated without special processing capabilities and therefore cheap, since they need only to transfer the collected data to the corresponding cluster-heads.

The second scenario on the other hand does not require an existing infrastructure deployed beforehand since clusters can forward data to other clusters similarly to multi-hop techniques, in order to reach the gateway. The leaders are responsible for relaying data to the gateway directly or via a number of intermediate leaders. The leader is dynamically selected according to its proximity to the gateway. This means that all nodes can and should be able to potentially become leaders. As a result, nodes need to have some computing power, and to be more sophisticated and more expensive than the ones employed in the first scenario.

In both scenarios, users' mobility may force them to leave their cluster and join a new one. The join procedure is triggered every time a node enters in the coverage area

of a new cluster. This implies that the underlying cluster-based routing algorithms need to adjust to this new topology and the group key management mechanisms will have to invoke re-keying procedures in order to assure backward secrecy and prevent the new nodes from accessing previous group communication. A similar procedure, namely leave, is triggered every time a node exits the coverage area of a cluster. In this case, group key management mechanisms will have to assure forward secrecy and prevent past cluster-members from accessing future communication. Group key management mechanisms should also cope with the case when the node that leaves the cluster is the leader. Dealing with the group key management, we assume that clusters located on the same floor use the same group key. We have chosen this approach instead of using a different group key per cluster, so that the displacement of patients within a small range not exceeding the boundaries of the floor where their rooms are located, will not affect group-key management. Therefore, re-keying procedures will not be triggered every time a node joins or leaves a cluster.

IV. GROUP-KEY MANAGEMENT

Group key management mainly includes activities for the establishment and the maintenance of a group key. A secret key for data encryption must be distributed with a secure and efficient way to all members of the group. Potentially, group key establishment is more suitable than pairwise key establishment as devices do not waste energy every time they wish to communicate with another device by establishing a new shared secret key.

In group key agreement protocols, all the nodes of the group collaborate and finally form a shared secret key. Key distribution techniques require a central authority or an on-line Trusted Third Party (TTP) to distribute the session keys which is not usually a realistic scenario in wireless ad hoc networks.

Group key establishment can be either centralized or distributed. In the first case, a member of the group is responsible for the generation and the distribution of the key. In distributed group key establishment all group members contribute to the generation of the key. Clearly, the second approach is well suited for ad hoc networks because problems with centralized trust and the existence of single point of failure can be avoided.

Most of the traditional group key management protocols reported in the literature can not cope with the dynamic nature and limitations of wireless ad hoc networks. In particular, the well known protocols appeared in [14], [15], [16] are efficient for wired networks but they can't be directly applied to ad hoc wireless networks. However, by organizing the nodes of the network hierarchically based on their relative proximity to one another and allowing the formation of small subgroups, this situation can change.

It has been proved in several works (e.g. [3], [4]) that clustering can improve the performance of traditional group key agreement protocols. In particular, in most of the cluster-based key agreement schemes, a general key agreement protocol is applied in every cluster and then the clusters' keys are used by the same or another key agreement mechanism to form the final group key.

In the context of this paper, we will propose the usage of several cluster-based key agreement protocols for our two different scenarios already discussed in section III, giving an abstract description for each one of them.

In the first scenario, a backbone network can be formed by the more powerful cluster-heads. We can follow two approaches: top-down or bottom-up. That is, in the first approach the cluster-heads can collaborate in order to construct a secret group key and then distribute it to their cluster members (e.g. as in [12]). In the bottom-up approach, a group key agreement protocol is applied in every cluster and then the different cluster keys are used in the backbone network for the establishment of the total group key. This can be achieved by either a group key agreement protocol in the backbone nodes [3], [4] or by using a protocol for cluster merging [17].

In our second scenario for medical environments, there is no backbone network or more powerful nodes. All nodes have equivalent resources and are organized in overlapping or non-overlapping clusters. Suppose that the clusters are put in several levels according to their distance from the gateway and that the root cluster is the closest cluster to the gateway. In order to construct a secret group key for the whole structure in the case that we have overlapping clusters, every cluster in the last level can generate a cluster key and then the nodes which belong also to the upper level can use it to form a key with the clusters of this level and so on until we reach the root cluster. Then, the group key constructed in the root cluster can be forwarded to the other clusters [18], [19]. The non-overlapping case can be considered as a special case of the overlapping one if we consider that the nodes which connect one cluster with another can form a separate, new cluster on their own. A different approach for this case will be the creation of different keys in every cluster and then a protocol for merging clusters [17] can be used for the construction of the final group key.

V. CONCLUSION AND FUTURE WORK

As WSNs have highly penetrated into the medical sector in a great degree due to their low cost, easy administration, flexibility etc the security issues namely confidentiality, integrity and availability need also to be confronted. Without doubt, security cannot be seen separately from the corresponding requirements for efficiency and scalability. Under these circumstances,

security mechanisms should also consider patients' mobility owing to be efficient and scale well every time new nodes join or leave the network. For security purposes, we also have to rely on some group-key management mechanisms.

Clustering solutions in terms of both routing and cluster-based group key management deal with the requirements for efficiency and scalability and therefore can also be envisioned in medical environments. In this context we have examined the cluster-based approach for the medical sector and proposed two different scenarios for in-hospital and e-emergency environments. We have also discussed group-key management schemes that can be profitably applied in our two scenarios.

As a future work we will further elaborate on WSN group-key agreement mechanisms in the context of the proposed scenarios. Specifically, our goal is to investigate, specify and evaluate key agreement mechanisms that will be custom tailored and thus particularly profitable to medical applications.

REFERENCES

[1] C. Karlof and D. Wagner, Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, *Elsevier's Ad Hoc Network Journal*, *special issue on sensor network applications and protocols*, 2002.

[2] G. Kambourakis, E. Klaoudatou and S. Gritzalis, Securing Medical Sensor Environments: The Codeblue framework case, *2nd International Conference on Availability, Reliability, and Security - 1st International Symposium on Frontiers in Availability, Reliability and Security*, R. Wagner, A.M. Tjoa et al. (Eds.), pp. 637-643, April 2007, Vienna, Austria, IEEE Computer Society Press.

[3] H. Shi, M. He, and Z. Qin, Authenticated and Communication Efficient Group Key Agreement for Clustered Ad Hoc Networks, in *5th International Conference on Cryptology and Network Security*, Lecture Notes in Computer Science Vol.~4301, Springer-Verlag, pp. 73-89, 2006.

[4] G. Yao, K. Ren, F. Bao, R. H. Deng, and D. Feng, Making the Key Agreement Protocol in Mobile Ad Hoc Network More Efficient, in *1st International Conference on Applied Cryptography and Network Security*, Lecture Notes in Computer Science Vol.~2846, Springer-Verlag, pp. 343-356, 2003.

[5] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan. Energy-Efficient Communication Protocols for Wireless Microsensor Networks, *In Proc. of the Hawaii International Conference on System Sciences*, Vol. 2, Maui, Hawaii, USA, January 2000.

[6] L. Schwiebert, S. Gupta, S. and J. Weinmann, Challenges in Wireless Networks of Biomedical Sensors, *SIGMOBILE 2001*, p. 151–165, July 2001.

[7] S. Dembeyiotis, G.Konnis and D. Koutsouris, A Novel Communications Network for the Provision of Medical Care in Disaster and Emergency Situations, *Proc. of the 24th EMBS/IEEE*, San Francisco, USA, Sep 2004

[8] D. Bottazzi, A. Corradi and R. Montanari, AGAPE: a location-aware group membership middleware for pervasive computing environments, *In Proceedings of the 8th IEEE International Symposium on Computers and Communication*, Kiris-Kemer, Turkey, IEEE Computer Society, Jun 2003, pp. 1185–1192

[9] F. Hu and S. Kumar, QoS considerations in wireless sensor networks for telemedicine, *In Proceedings of SPIE ITCOM Conference*, Orlando, FL. 2003

[10] J. Misic and V. B. Misic, Implementation of security policy for clinical information systems over wireless sensor networks, *Elsevier's Ad Hoc Networks*, vol.5, no.1, Jan 2007, pp.134-144.

[11] F. Hu, J. Tillett, J. Ziobro, and N. K. Sharma, Secure Tree-Zone-Based Wireless Sensor Networks for Telemedicine Applications, *in Proc. of IEEE GLOBECOM*, 2003, pp. 345–349.

[12] Y. J. Chen, Y. L. Wang, X. P. Wu, and P. D. Le, The Design of Cluster-based Group Key Management System in Wireless Networks, *International Conference on Communication Technology - ICCT'06*, 2006.

[13] A. Youssef, M. Younis, M. Youssef, A. Agrawala, Distributed formation of overlapping multi-hop clusters in wireless sensor networks, in: *Proceedings of the 49th Annual IEEE Global Communication Conference*, San Francisco, CA, November 2006.

[14] M. Burmester and Y. Desmedt, A Secure and Efficient Conference Key Distribution System, in *Advances in Cryptology* - EUROCRYPT 1994, Lecture Notes in Computer Science Vol.~950 (Springer-Verlag, 1994), pp.275-286.

[15] Y. Kim, A. Perrig, and G. Tsudik, Tree-based group key agreement, in *ACM Transactions on Information and Systems Security*, vol. 7, no. 1, pp. 60-96, 2004.

[16] M. Steiner, G. Tsudik, and M. Waidner, Diffie-Hellman Key Distribution Extended to Group Communication, in *Proceedings of 3rd ACM Conference on Computer and Communications Security*, ACM Press, pp.31-37, 1996.

[17] S. Shin and T. Kwon, Efficient and Secure Key Agreement for Merging Clusters in Ad-Hoc Networking Environments, IEICE Trans. Commun., Vol. E90-B, No. 7, July 2007.

[18] A. Abdel-Hafez, A. Miri, and L. Oronzo-Barbosa, Authenticated Group Key Agreement Protocols for Ad hoc Wireless Networks, *International Journal of Network Security*, Vol. 4, No. 1, pp. 90-98, 2007.

[19] Y. Chen, M. Zhao, S. Zheng, and Z. Wang, An Efficient and Secure Group Key Agreement Using in the Group Communication of Mobile Ad-hoc Networks, in International Conference on Computational Intelligence and Security, pp. 1136 - 1142, IEEE Press, 2006.