A Secure Communication Protocol for Wireless Ad Hoc Network

Amar S. Ingle[1] Prof. S. U. Nimbhorkar[2]
[1,2]Department of Computer Science & Engineering
[1,2]G.H. Raisoni College of Engineering, Nagpur, India

Abstract— In recent year, progress in wireless technology reach at higher level as the more portable mobile devices are equipped with such technology, monitoring and controlling is flexible by using these technology , the exponential growth and development in the wireless communication, Wireless communication technology can be used in extreme condition in very effective approach. Wireless ad hoc network is one of the efficient medium for mobile communication having facility for the sharing of resources and it introduces new services among the user. Thus the host communication in the wireless network must be in a secure way. Such type of network is self-implemented which able to create the network on basis of sharing various services without any large network setup. It uses integrated symmetric and initial trust between users for exchanging the initial data packets and secret keys which is used for encryption and decryption of incoming and outgoing data packets. The primary validation is based on the initial key distribution among the network users and re-authentication is made after a new session start to secure the network. For security analysis of the system and highlights the features of a secure protocol comparison is made between other ad hoc network protocols.

Key words: secure protocol, wireless ad hoc network, clustering methods, encryption, secure data transmission

I. INTRODUCTION

Wireless technology is very important aspect in many fields due to easy deployment; user mobility involves several functionalities such as providing information anywhere, user sociability, strength, scalability and elasticity of wireless communication increases user's efficiency and flexibility. Wireless ad hoc network is nothing but a set of portable terminals placed in a specified range in which terminals can be able to communicate with each other with the help of wireless link. Proposed secure procedure is designed for unplanned wireless ad hoc network which uses a hybrid symmetric and asymmetric scheme [1]. A various security scheme provides a completely independent Protocol and it will help to share secured services without any infrastructure by creating a new network [2] [3].Proposed protocol includes all the functions needed to operate wireless network as standalone network without any peripheral support.

Wireless ad hoc network is made from a combination of mobile terminals placed in a close location that are able to communicate with each other, sharing resources and services. In a several protocols researchers consider only wireless spontaneous networks and initial authentication only [1][4][7],but when we have only initial authentication and in that case if certain elected node in the network leave the network and at same time if attacker make duplicate copy of it then it may causes a security damage to the network. Our objective is to integrate the services and devices in such way that they do a secure communication in the wireless ad hoc environment.

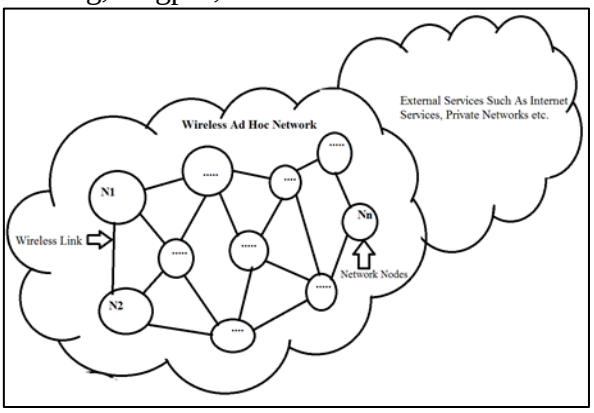

Fig. 1: Wireless Ad Hoc Model

As the wireless ad hoc is an emerging technology it requires efficient security mechanism [26], and such secure mechanism helps to protect data integrity. The basic steps in the security mechanism include user recognition, their permission, and address assignment, identification service, procedure and safety. None of the existing papers proposes such a communication protocol for Wireless Ad Hoc Network based on such a protected schemes [21].

In this protocol first we will do clustering with the help of K-Means Algorithm and other efficient methods, if we have a new node present in the network then we do new node addition with the help of SET-IBS protocol mechanism [9] [12] [16], then Inter network communication with the help of ECC algorithm which is cryptology algorithm and used for the encryption and decryption of message over a wireless Ad hoc network. By considering the above scenario the modules of the application also get divided in related way. We consider the network stimulator environment for testing our protocol.

Wireless ad hoc network is also called as the impulsive ad hoc network because it created spontaneously when we needed. Wireless ad hoc network is mutihop network having self-configured, self-optimized data network because it separate from the other external networks [21]. So security issues are the main challenges for the wireless ad hoc network communication. A secret key management scheme can be used to encode and decode the incoming and outgoing data respectively in this network communication and with help of it the data in the network is protected from external attackers. Session initiation protocol is used to connect the ad hoc network to the external networks to access various services. But the communication established to the external network should be secure. Various security schemes can be used to defend the ad hoc network from the external attack. Figure 1 shows the typical architecture of wireless ad hoc network having communication nodes with wireless links and establishing connection between network nodes.

II. LITERATURE REVIEW

There are various methods which have been used for securing and monitoring wireless ad hoc network. This will

be helpful for introducing an integrated secure protocol for the wireless ad hoc network. Raquel Lacuesta uses the hybrid symmetric or symmetric schemes which include the initial data exchange on basic of user's reliance. In this paper reliance is based upon the first visual contact. The proposed system having the autonomous protocol which helps in secure communication in network node and also it do not need any large infrastructure [1].

Zygmunt J. introduces a secure and self-automated fault tolerant communication network as the design of the network change. Here paper proposed a protocol to evaluate the malicious disruption of the data in the message transmission they called it as the secure transmission protocol and secure single path protocol [2] but these protocols are run solely on the trust basic of the network and security associations. As the result of this the network may having the security issues as any malicious node is present in the network.

As wireless ad hoc nodes having mobility it causes frequent changes in the topology of a network. If certain node moves out of radio range of network then link is broken such types of networks are very useful for the defence purposes [3], but when the link is broken down then reorganized node data must be updated on the base station of wireless ad hoc network for the security concern.

Zhiguo Wan [4] shows the demand of the secure routing protocol for the mobile ad hoc network as the privacy of certain networks is fundamental requirement. Juhani latvakoski [5] Present a communication Architecture for Spontaneous Systems in this papers author take communication types as peer to peer, there no specific security scheme is going to define by the author. When the ad hoc nodes which is mobile it must have a several security schemes for the secure communication between the nodes, and in [6] implementation of the cellular mobile network is shown, it may be used in the ad hoc network.

Chi Zhang design a identity based cryptosystem which delivers necessary security requirements to the network Ad hoc network is more significant way that other network cannot able to attack on the network [7] and the challenging issues are discuss in [8], As the ad hoc network having the self-structured mechanism and key management is one of the important part of it and for the encryption algorithm a public key management technique is introduced in ad hoc network [9]. Ad hoc network forms the cluster on the basic of their geological location or energy constraints we may take another parameter for it. In [10] proposed the two protocols for the secure data transmission in the cluster based ad hoc network.

A distributed approach proposed for dynamic cluster formation and management [11], in this paper authors are used the triangular approach to search the new mobile node present near to the groups nodes of a wireless network. Emiliano Garcia-Palacios Proposed a secure cluster head election mechanism, the cluster head is acts a monitor of the entire cluster [14]. When we need more improvement in the clustering methods of the wireless ad hoc network then researchers reconsider relative performance of the re-clustering algorithms in the movable ad hoc network [15]. As the data communication in the ad hoc network is done in a secure way then for the encryption and decryption researchers proposed a safe and sound cluster base key management technique [19] which uses distributed authorities and also proposed a robust re-clustering algorithm.

III. Proposed Methodology and Discussion

In the proposed system, Our protocol Specially design for the wireless ad hoc network which is standalone network where all the service of the network are self-configured by the network users and nodes for the secure transmission of the data, Here we considered n nodes in the network which is nothing but the network user which are going to share the network resources and take part in the network communication. We used k-means algorithm for initial cluster formation and on the basic of their geological location we elect the base station in the on network we have several group of wireless ad hoc network and which are connected with the direct link between the respective base stations. In clustering module we are going to create the node by using the k-means cluttering algorithm, we have base station in ad hoc network for centralized control, which gives various services to the cluster heads in the network. Cluster head elected in the network on the basic of their energy level or geological position. We may elect Dynamic cluster head on the basic of their energy levels for network stability and robustness for certain conditions, If cluster head lost energy then it will switch to another cluster head which having high amount of energy in this scenario we may consider take other parameter for the cluster formation in network.

We proposed an efficient technique which is able to do clustering of network with respective to their correlation; we used Data Density Correlation Degree Clustering Method [20] in an efficient way to do the clustering in this protocol. We do the cluster head election means we have the cluster head for each cluster and in the network there is one or more clusters, here cluster head is equal to the number of clusters present in the network.

Consider there is C clusters are present in the network and CH are the cluster head present in the network, the mathematically we represent it as C = CH, we used various protocols which are prior implement by the researchers to setup the communication link between the network nodes. Here, several types of communication in the ad hoc network that are; one base station to another base station, base station to cluster head and cluster head to cluster nodes. We used cryptosystem for the encryption and decryption of data which is based upon the ECC to fulfill the purpose of the secure communication in the network.

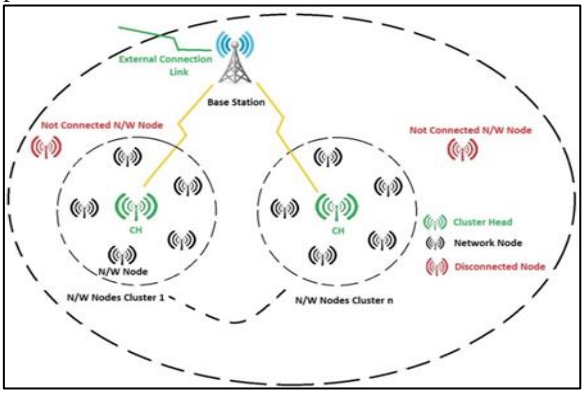

Fig. 2: System architecture

Figure 2 describe the overall architecture of the propose system. Here Base Station monitors the centralized communication in the wireless ad hoc network, which is connected to the cluster head through wireless link. In this Wireless system mainly we have three types of nodes i.e. Network Node, Cluster Head and Disconnected Node. Network nodes are the members of the particular cluster, which are further connected to the cluster head for the secure communication of the data in the network. For each cluster we elected cluster head, which monitor the communication in the cluster by forming a communication link with each cluster and directly connected to its base station. In this system disconnected nodes are the nodes of the network which are not authorized to use the services of the network.

We used the network stimulator ns2 for implementation of this integrated protocol. We initially setup environment of mobile nodes which is having a fixed base station for the centralized control, after that we do the clustering process by using K-means algorithm for the cluster formation. Each cluster of the wireless network having its cluster head and it monitors the communication at cluster level and formed a communication link to base station. Figure 3 Shows the basic communication flow of the Proposed system, In the proposed system consist of three system module which is shown in figure 3, first module in for the creation of clusters for the group communication; second module is for the addition of the new node in the network and the third module is for the inter network communication. The basic working Steps in Secure Wireless Ad Hoc network are:

1) Clustering Process by Using K-means algorithm
2) New Node Addition to Cluster and Services discovery
3) Inter Network Communication with ECC Based Cryptosystem
4) External Network Communication

In the First module we do the clustering of the network nodes on the basic of their geological location we introduced K-means algorithm to ensure this scheme in the system. By using k-means algorithm we formed a several cluster in the network and each cluster having its cluster head. In the service discovery module of the project we will show the communication between the network nodes of the wireless ad hoc network. In this module the network node of each cluster sending the packets to respective cluster for the service discovery and a communication link is formed between the nodes here unauthorized packets rejected by the cluster head. We proposed an efficient technique which is able to do clustering of network with respective to their correlation; we used Data Density Correlation Degree Clustering Method in an efficient way to do the clustering in this protocol. We do the cluster head election means we have the cluster head for each cluster and in the network there is one or more clusters, here cluster head and equal to the number of clusters present in the network.

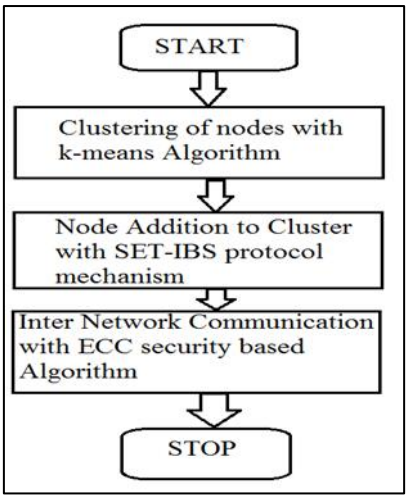

Fig. 3: Flowchart of Proposed Design

In the Establishing Trusted Chain and Changing Trust Level Module of the project we are forming the secure chain of communication by using the ECC Cryptography and SET-IBS Protocol Schemes. In this we are going to use the ECC algorithm for the encryption of data. When cluster head is going send the data to the BASE station it's in the encrypted format for maintaining the data integrity. In this we used the ECC protocol at every cluster head that means our cluster head receive data from non-cluster head and send to base station by encrypting that data with ECC protocol. We also calculate the time taken by ECC for encrypting the data in millisecond as per data size.

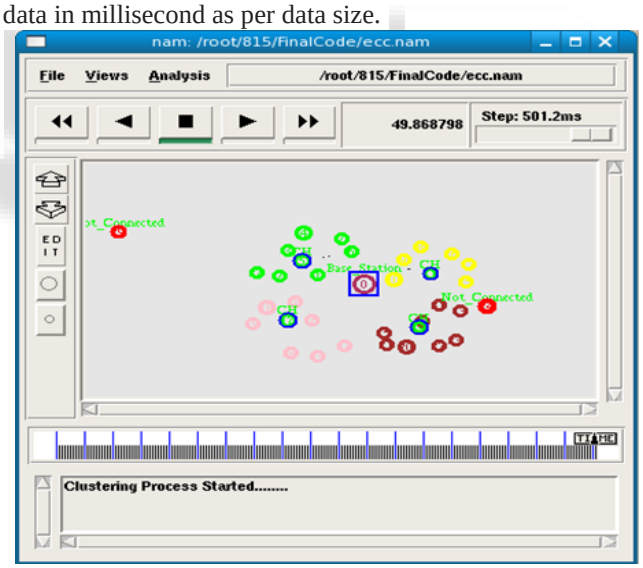

Fig. 4: Simulated Network Setup for Wireless Ad Hoc Network.

Figure 4 show the simulated network setup for the wireless ad hoc network which shows the network nodes present at one base station.here we have the several clusters and each cluster having its own cluster head which link to its respective cluster nodes and base station.

IV. Results and Analysis

All the results are going to show on the network simulator ns2.we are going to use the xgraph functionality in ns2 for showing the stimulator results. In the xgraph we consider the time as the main parameter as link this parameter with the other respective parameters and evaluate the graph for the system, we made the comparison between the proposed

system and the existing system. We are going to dealing with the security issues in the wireless Ad Hoc network. We consider ECC algorithm as the main aspect. In the previous system researchers use the RSA algorithm for providing security to the wireless Ad Hoc network, but RSA security is not up to the mark for providing security services to the wireless Ad Hoc network. So by considering various aspects we are going to integrate ECC algorithm to this protocol. We setup a same environment for existing system and previous system, here same environment refer as the similar parameters for the wireless Ad Hoc network. We firstly consider 35 network nodes under the single base station and run the stimulation on ns2.

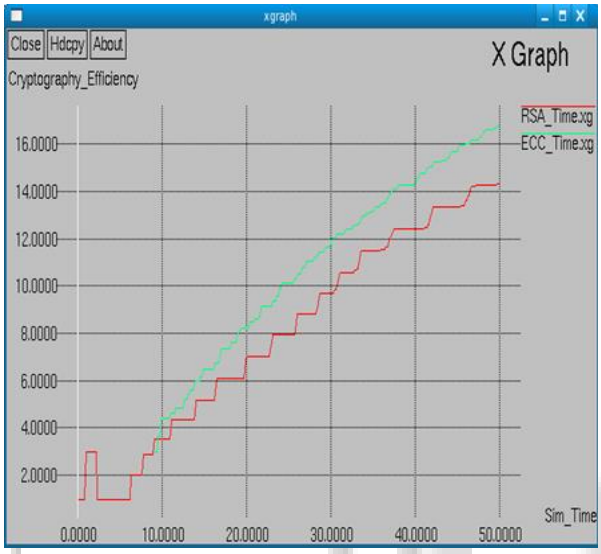

Fig. 5: Cryptography Efficiency

So we got the following stimulated results.

1) Network Delay and Throughput.
2) Performance of the encryption.
3) Packet Delivery Ratio of the network.
4) Energy consumption of both networks.
5) Communication overhead
6) Packet loss during the data transmission

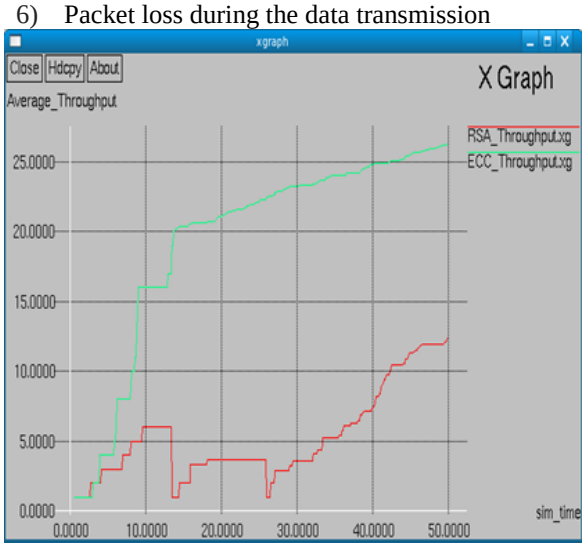

Fig. 6: Average Throughput of the System

In Figure 5 and Figure 6 show the System Comparisons on the basic of ECC and RSA Cryptography, in figure 6 graph shows ECC cryptography efficiency is more than RSA and our ECC based system having maximum throughput than previous RSA based Security protocols. We get maximum the Packet delivery ratio for the existing system.

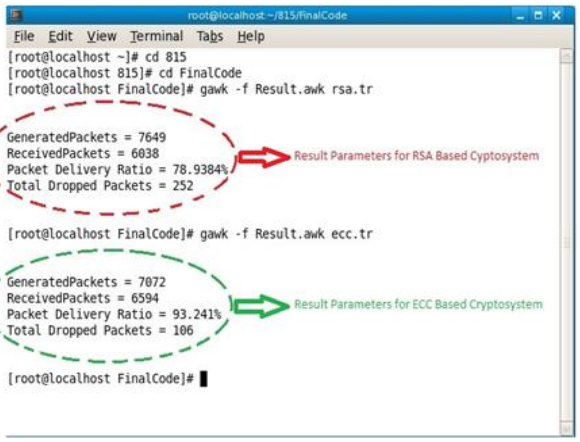

Fig. 7: Results Parameters of the System

By comparing all the above results we are going to conclude that our proposed system perform well as compare to the previous system and provides security services for wireless Ad Hoc Network by using elliptic curve cryptography which having low communication overhead.

V. CONCLUSIONS

This paper proposes a secure data communication protocol for the wireless ad hoc network that allows creating and managing the wireless ad hoc network in a secure way. This protocol can be used in defence purposes and many other areas where data security and privacy on a top priority. We used various algorithms and techniques to form clusters in the network and for achieving centralized control over the network we elected the based station of a network and cluster head of each cluster in the network. We introduced protocol in the user responsive background for the easy access. The security schemes used in this protocol ensures the secure communication over the wireless ad hoc network.

REFERENCES

[1] Panagiotis Papadimitratos, Member, IEEE, and Zygmunt J. Haas, Senior Member, IEEE, "Secure Data Communication in Mobile Ad Hoc Networks" IEEE Journal On Selected Areas In Communications, Vol. 24, NO. 2, Feb 2006.

[2] Lidong Zhou and Zygmunt J. Haas Cornell University, "Securing Ad Hoc Networks" IEEE transactions on Network November/December 1999.

[3] Zhiguo Wan, Kui Ren, and Ming GU,"USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks" IEEE transactions on Wireless Communications, Vol. 11, No. 5, May 2012.

[4] Juhani Latvakoski, Danielpa Kkala, and Pekka Paakkonen, Vtt Technical Research Finland Kaitovayla, "A Communication Architecture for Spontaneous Systems" IEEE Wireless Communications- June 2004.

[5] Marc Danzeisen , Torsten Braun, Simon Winiker, Daniel Rodellar, "Implementation of a cellular framework for Spontaneous Network Establishment" IEEE Communications Society / WCNC 2005.

[6] Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang, Fellow, IEEE, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks" IEEE transactions on Parallel And Distributed Systems, Vol. 21, No. 9, Sept 2010.
[7] Sudeep Thepade, Rik Kamal Kumar Das, "A Study of Transport Protocols For Wireless Ad Hoc Networks" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-4, April 2012.
[8] Srdjan Capkun, Student Member, IEEE, Levente Buttya´ n, Student Member, IEEE, and Jean-Pierre Hubaux, Senior Member, IEEE, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks" IEEE transactions on mobile Computing, Vol. 2, no. 1, Jan-March 2003.
[9] Huang Lu, Student Member, IEEE, Jie Li, Senior Member, IEEE, Mohsen Guizani, Fellow, IEEE, "Secure and Efficient Data Transmission for Cluster-based Wireless Sensor Networks" IEEE transaction on Parallel and Distributed systems, 2012.
[10] A. Selva Reegan, E. Baburaj "Key Management Schemes in Wireless Sensor Networks: A Survey" 2013 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2013].
[11] Emiliano Garcia-Palacios, Noureddine Mehallegue, and Ghazanfar Ali Safdar,"Providing Security and Energy Efficiency in Wireless Ad-Hoc sensor Networks through Secure Cluster-Head Election (SEC-CH-E)" IEEE 2012.
[12] C. Tselikis, C. Douligeris, S. Mitropoulos, N. Komninos, "Consistent Re-clustering in Mobile Ad Hoc Networks" IEEE 2008.
[13] Melaku Tamene ,Kuda Nageswara Rao,"Grid based Clustering Protocol with Dynamic Range Cluster head Advertisement and Traffic Splitting in Wireless Sensor Networks" IEEE 2011.
[14] K. Gomathi, Dr.Meera Gandhi "Weight based Clustered Key Management scheme using RSA for Wireless Mobile Ad hoc Networks" IEEE-ICoAC 2011.
[15] Xiaoyan Wang, Student Member, IEEE, Jie Li, Senior Member, IEEE, and Feilong Tang, "Network Coding Aware Cooperative MAC Protocol for Wireless Ad Hoc Networks" IEEE transactions on Parallel and Distributed Systems, vol. 25, no. 1, Jan 2014.
[16] Lung-Chung Li and Ru-Sheng Liu, "Securing Cluster-Based Ad Hoc Networks with Distributed Authorities"IEEE transactions on Wireless Communications, Vol 9, No. 10, Oct 2010.
[17] E. Hemalatha Jai Kumari, Kannammal. A "Analysis of Security Algorithms towards secured communication in Wireless Networks" ICCCNT 2012.
[18] C. Tselikis, S. Mitropoulos, Senior Member, IEEE, N. Komninos, Senior Member, IEEE, and C. Douligeris, Senior Member, IEEE "Degree-Based Clustering Algorithms for Wireless Ad Hoc Networks under Attack" IEEE Communications Letters, Vol. 16, No. 5, May 2012.
[19] E. Hemalatha Jai Kumari, Kannammal. A "Energy analysis of Public-Key Cryptography for Wireless Sensor network" ICCCNT 2012.
[20] Amar S Ingle, S.U. Nimbhorkar "A Review on Secure Communication Protocol for Wireless Ad Hoc Network" IEEE International Conference on Pervasive Computing (ICPC), pp. 1-4, Feb 2015
[21] T. Hara, V.I. Zadorozhny, and E. Buchmann, Wireless Sensor Network Technologies for the Information Explosion Era, Studies in Computational Intelligence, vol.278. Springer-Verlag, 2010.
[22] S. Xu, Y. Mu, and W. Susilo, "Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security," Proc. 11th Australasian Conf. Information Security and Privacy, pp. 99-110, 2006.
[23] K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," Proc. Fourth Int'l Conf.Wireless Comm., Networking and Mobile Computing (WiCOM), pp. 1-5, 2008.
[24] A.A. Abbasi and M. Younis, "A Survey on Clustering Algorithms for Wireless Sensor Networks," Computer Comm., vol. 30, nos. 14/ 15, pp. 2826-2841, 2007.
[25] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," Proc. Advances in Cryptology (CRYPTO), pp. 47-53, 1985.
[26] S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Signatures," Proc. Advances in Cryptology (CRYPTO), pp. 263-275, 1990.
[27] J. Liu et al., "Efficient Online/Offline Identity-Based Signature for Wireless Sensor Network," Int'l J. Information Security, vol. 9, no. 4, pp. 287-296, 2010.
[28] K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," Proc. Fourth Int'l Conf.Wireless Comm., Networking and Mobile Computing (WiCOM), pp. 1-5, 2008.
[29] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Comm. Surveys & Tutorials, vol. 8, no. 2, pp. 2-23,Second Quarter 2006.
[30] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "AnApplication-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660- 670, Oct. 2002.

