A Secured Dynamic Cluster-Based Wireless Sensor Network

L. B. Jivanadham[1], *A.K.M. M. Islam[2]
[1]*Advanced Informatics School (AIS)*
Universiti Teknologi Malaysia (UTM)
54100 Jalan Semarak, Kuala Lumpur, Malaysia
[1]bjlalitha2@live.utm.my
*Corresponding Author: [2]akmmislam@ic.utm.my

N. Mansoor[3], and S. Baharun[4]
[2,3,4]*Malaysia-Japan Int'l Institute of Technology (MJIIT)*
Universiti Teknologi Malaysia (UTM)
54100 Jalan Semarak, Kuala Lumpur, Malaysia
[3]nafees@nafees.info
[4]drsabariah@ic.utm.my

Abstract— **Driven by the technology advances in Micro-Electro-Mechanical Systems which has facilitated the development of smart sensors; we have witnessed in recent years the emergence of WSNs in environment, military, surveillance, natural disaster relief, healthcare, etc. These WSNs carry the promise of drastically improving and expanding the quality of services across a wide variety of settings and for different segments of the population. Therefore, it is very important to develop a WSN with robustness and security in mind. Typically, the sensors are smaller in sizes that have limited processing and computational power resources, and are inexpensive, thus enabling the network to have a large coverage area and longer range. By using hundreds or thousands of them it is possible to build a high quality, fault-tolerant sensor network where failure of one or few nodes does not affect the operation of the network. They are also self-configuring or self-organizing. In this paper, we propose formation of a Secured Cluster-based architecture for a Dynamic Wireless Sensor Network that uses two topology management operations: node-move-in and node-move-out. The proposed security protocol integrates one round Zero Knowledge Proof and AES algorithm to apply for node authentication, where only authenticated nodes will be accepted during node-move-in operation. We also show that it requires *O(h+q)* rounds for a node to join into a network securely, where *h* is the height of the dynamic cluster-based wireless sensor network and *q* is the number of neighbouring nodes of a joining node.**

Keywords-wireless sensor networks; security; dynamic wireless sensor network; node-move-in; node-move-out; node authentication; zero knowledge proofs; dynamic cluster based WSN;

I. INTRODUCTION

Great attention has been given in the field of Wireless Sensor Networks (WSNs) in recent years due to its substantial advances in wireless and mobile communication techniques and the broad development of potential applications. Wireless Sensor Networks (WSNs) comprises hundreds and thousands of sensor nodes deployed to undertake a particular mission such as habitat monitoring, agricultural farming, military [1] and in rescue missions in a catastrophe. It is made up of a collection of application specific sensors, a wireless transceiver, a simple general purpose processor, possibly assisted by limited amount of special-purpose hardware, and an energy unit that may be a battery or a mechanism to obtain energy from the environment [2]. Sensor nodes in the network are tiny, inexpensive and resource constraint devices as shown in Fig. 1. They have limited memory, computational capacity, limited transmission range and having limited energy as well. Sensor nodes are distributed over a potentially vast geographical area to provide a non-centralized, self-organizing, dynamic topology and multi-hop routing [3-5].

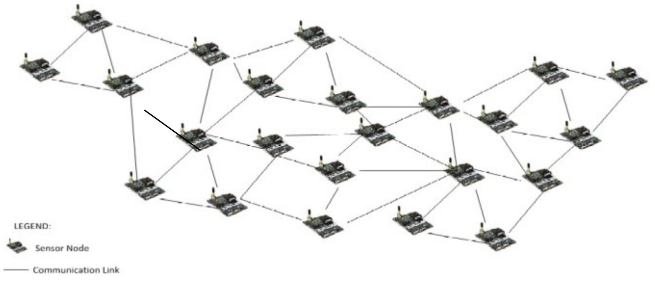

Fig. 1: Example of a Wireless Sensor Network (WSN)

By having a non-centralized architecture WSNs allows any node to join or disjoin the network at any time due to its lack of a central administration [1-6]. In addition every node in the network has identical status that no one node is responsible for providing services to each other. The failure of some nodes in the network does not affect the whole sensor network; in fact this makes the network more reliable for applications with high stable requirements.

WSNs are known for its self-organizing ability as they are characterized as infrastructure-less networks and lack of fixed infrastructure. When a set of sensors begin working with some pre-defined layering protocols and distributed algorithms the sensor network is established due to its ability to self-construct. By establishing the sensor network, sensed data is collected and send to back-end system for further processing through the networks built.

WSNs can be deployed in several topologies depending on its organizational practices, policies and usage utilities. Common topologies found in wireless sensor networks are flat/unstructured topology, cluster oriented topology, hierarchical topology and chain oriented topology. Since the sensors in sensor networks might shut down, crash, recovery or utilize mobile sensors these nodes are deployed randomly and the network topology changes dynamically.

As sensor nodes have limited transmission range, the sensor range in WSNs is expected to be limited as well. Therefore, WSNs is said to provide multi-hop routing where, if node *u* would like to communicate with node *v*, which is out of the communication range, an intermediate node *w* is required to facilitate this communication. Node *w* is responsible for transmitting the communication data from node *u* to node *v*.

The existing communication schemes show that there are three main types of communications in WSNs including data gathering, routing and broadcasting communication. Multi-hops communication is used because the communication range of a sensor is assumed to be limited and the neighbouring sensor nodes maybe used for transmitting the communication packets to each other on their path between the source node and the destination node.

The conflicting interest between minimizing resource consumption and maximizing security is a major dilemma in DCWSN environment. Any security mechanisms for DCWSN must consider the five major resource constraints that are the limited energy, limited memory, limited computing power, limited communication bandwidth and limited communication range. However, the capabilities and constraints of sensor node hardware will also influence the type of security mechanisms that can be hosted on a sensor node platform.

The rest of the paper is organized as follows. Section II elaborates the related works. Followed by Section III describing the selected network architecture, then our proposed security protocol in Section IV and finally in Section V, the conclusion and future work on this work is given.

II. Related Works

In [11], a novel Cluster-Based Architecture for a Dynamic WSN is presented. To perform an efficient broadcasting the architecture constructs and maintains a Communication Highway named as *Backbone Tree (BT)*. The paper also proposed maintenance algorithms for the architecture. Later in [12], an improved cluster- based architecture with reduced BT height is proposed to support a better broadcasting and efficient multicasting algorithms. Thereafter in [13], another novel cluster-based architecture and a designed a Communication Super Highway called *Super Backbone Tree (SBT)* is suggested to facilitate an efficient routing algorithm. In that article, the proposed size of SBT is smaller than that of BT. However, there is a deficiency in the proposed routing algorithm since it creates routes on the SBT instead of graph *G*. Thus in [13], a further improved routing algorithm that creates paths on graph *G* is authored. Finally in [14], another novel cluster-based architecture is proposed where the authors have reduced the size of BT significantly. Here it is presented that node-move-in and node-move-out on this architecture can be done efficiently. Based on the above works it is clear that the vital aspect of any network which is the security feature is missing in this clustered architecture.

On the other hand, different systems may require different types of credentials to determine user identity where credential is the evidence or documentation provided by a user in the process of user authentication. Credentials may take other forms, including PIN numbers, certificates and tickets. Though there are many authentication schemes that may possibly applied to WSNs including password, challenge-response method with keyed hash functions, asymmetric-key cipher and digital signature, in this paper we are focusing on the Zero Knowledge Proof (ZPK) scheme. As discussed in the earlier section, the WSNs have limitations and these limitations complicate the security design and deployment in sensor networks. This is the main reason why we have considered paying attention to the ZPK scheme for authentication.

A Zero Knowledge Proof (ZKP) protocol is a powerful cryptographic system that can be applied in many cryptographic applications and operations such as identification, authentication and key exchange is elaborated in [15]. The uniqueness of ZKP is that the claimant protects the confidentiality of the secret at any cost by not revealing anything. The framework of ZKP is described in [16] where the claimant is responsible to proof she knows a secret, without revealing it to the verifier.

The first protocol analyzed is the Fiat-Shamir Protocol in [17].The other ZKP protocol studied is the Feige Fiat Shamir Protocol which is similar to the first approach [17] except that it uses a vector of private keys, a vector of public keys and a vector of challenges. In this protocol the claimant proves their identity to verifier using *t* rounds of a 3-step protocol. In order for an entity *A* to use this protocol, some setup is required. Finally, the Guillou-Quisquater Protocol [18] is also a ZKP that is an extension to Fiat-Shamir protocol in which fewer numbers of rounds can be used to prove the identity of the claimant.

Most of the wireless sensor network uses the symmetric key schemes because these schemes consume less computation time than other schemes. The ingredients of a security protocol are cryptographic algorithms, which are selected based on the security objectives that are to be achieved by the protocol. Parameters like the size of the plaintext and cipher text, the implementation complexity of the algorithm and the key scheduling determines the cost of encryption and decryption in a security protocol. Specifically, key length is important and the longer the key the higher the encryption time. Also, the cost for decryption depends on the cost of the checks needed to accept the decryption.

Based on the key distribution, key discovery and key establishment in the schemes, we divided these schemes into six categories: entity based schemes, pure probabilistic-based schemes, polynomial-based key pre-distribution schemes, matrix- based key pre-distribution schemes, tree-based key pre-distribution schemes and EBS-based key pre-distribution schemes [19]. Entity based schemes or arbitrated schemes are those schemes in which key distributions and key establishment are based on trusted entity. Master key based pre-distribution scheme is discussed in [20]. In this scheme, a master key is pre-distributed and stored in each sensor in the network. A pairwise key can be established by using this master key and a random number exchanged between each sensor. In [21] this scheme has infinite scalability and each sensor only needs very little memory. However, when the master key is compromised; all the pairwise keys are exposed. Apart from that, there is no authentication as all the sensors have the same master key. An improved scheme is that the master is erased after the pairwise keys are established based in [22].

The implementation of AES-Rijndael on sensor networks has two major concerns which are highlighted in the literature of [23-25]. In these articles AES-Rijndael is considered too slow and it requires more space in memory. In fact, the baseline version of AES-Rijndael uses over 800 bytes memory space for lookup tables, which is a high overhead on constrained WSN environment. However some researchers do believe that Rinjdael can be efficiently implemented on WSN platform as stated by Vitaletti and Palombizio in [24] where an improved implementation of AES-Rijndael for wireless sensor networks running on Eyes sensor nodes is presented. Finally in [26], the authors have proposed and recommended the use of low power AES crypto at the systems which have resource constrained environments like the WSN.

III. Dynamic Cluster-based Wireless Sensor Network

The basic idea of clustering is to break the flat topology network into physical proximity clusters as shown in Fig. 2a and Fig. 2b. The clusters are smaller than the network as whole and therefore easier to manage. In DCWSN topology (Fig. 2c), nodes are classified as cluster head (CH), gateway and pure member (PM). Each cluster is managed around cluster heads (CH). Gateway (GW) is the node that connects two clusters. The following definition gives the construction of the clustering in DCWSN.

Definition 1: Given a graph G = (V, E) with a specified node r, a cluster-based network of G, called as cluster-based network of G and denoted as CNet(G), is a spanning tree of G with root r. In CNet(G), each node knows its status: either as cluster-head, or as gateway, or as pure member node. CNet(G) can be defined recursively as follows: If G contains one node r, then r is the root of CNet(G) and r is a cluster-head.

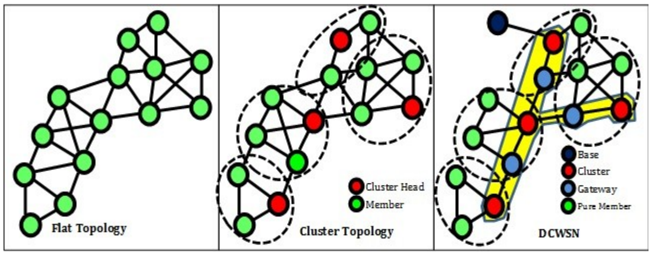

Fig. 2: Formation of DCWSN (a) Flat Topology (b) Clustered Topology (c) DCWSN

Subsequently, the clustering induced hierarchy is used in the construction of Backbone Tree (BT) to form a structure that mainly consist of CHs and gateways that provides efficient communication between the clusters [11].

The dynamic cluster based wireless sensor network is selected as the architecture to implement the proposed security protocol due the benefits it offers compared to the flat topology. This structured network is responsible in providing desirable properties such as minimized communication overhead, choosing data aggregation points, increasing the probability of aggregating redundant data and minimizing the overall power consumption. The WSN can be represented by graph where the sensors deployed in the network is represented by the vertex and the communication links between sensor nodes are represented by the edges joining the vertices as illustrated in Fig. 2a, 2b and 2c [11].

In this architecture model, we introduce Base Station (BS). The Base station acts as the controller; it is secured and has powerful resources in terms of energy, computation and memory compared to all the other sensors in the network. The base station is introduced because the nodes in the existing architecture have limited resources in terms of computation and energy. However, as the need for a secured DCWSN emerges it is also a huge challenge in designing a security protocol for WSNs to provide high-security requirements with these constrained resources.

The security requirement for DCWSN in this paper covers node authentication, confidentiality, integrity and communication and resources efficiency. To identify both trustworthy and unreliable nodes from a security standpoint, the deployment sensors must pass node authentication examination by their corresponding manager nodes or cluster heads and unauthorized nodes can be isolated from WSNs during the node authentication procedure. Similarly, all the packets transmitted between a sensor and the manager node must be kept secret so that eavesdroppers cannot intercept, modify and analyse, and discover valuable information in WSNs.

IV. Proposed Security Protocol

Security plays a very important role in WSNs which mainly includes: authentication and key establishment. The primary goal of an authentication scheme is to prevent unauthorized users from gaining access to protected system [7-8]. Since WSNs uses shared wireless medium, authentication is a necessary procedure for verifying both an entity's identity and authority. With the node authentication an invalid node will be unable to send malicious data into the networks and the manager node is able to determine whether received sensed data has come from a valid sensor node, and not from unrecognized nodes. This also indicates that sensor nodes that join a WSN have been validated and it has the right to access the sensor network. Without node authentication, an adversary can masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes. Moreover a compromised node may send data to its aggregator under several fake identities so that the integrity of the aggregated data is jeopardized [9-10]. However, engineering good authentication protocols for sensor networks carry an extra burden of anonymity requirements. It is imperative that authentication protocols release as little information as possible relating to the principals involved in the protocol execution.

In most mission critical applications, sensor nodes transmit highly sensitive data like secret keys, public keys and sensor identities which makes it extremely important to construct secure transmission path among these nodes. Data confidentiality is a key attribute that ensures the secrecy of sensed data and is never disclosed to unauthorized parties. Furthermore, routing information must also remain confidential as in certain cases malicious nodes may use the sensitive data secret to encrypt the data with a secret key that only intended for the receivers' possess.

Although data confidentiality guarantees that only intended parties obtain the un-encrypted data, but this data is still exposed to alteration. Data integrity ensures that a message transmitted is never corrupted. In order to prevent network from functioning properly, a malicious node may just corrupt messages transmitted in this network. In fact, due to unreliable communication channels, data may be altered without the presence of an intruder. Providing data integrity is not enough for wireless communications because sensor nodes are able to listen to transmitted messages and replay to disrupt the data aggregation results.

The secured DCWSN integrates the one round Zero Knowledge Schemes and Advance Encryption Scheme (AES) based on to their simplicity, strong security and relatively low computational requirements minimum-knowledge schemes are ideally suited for microprocessor based devices where the processing power and storage capacity is limited. Thus, this has become the motivation behind the adaption of Zero Knowledge Schemes for node authentication and symmetric key establishment for securing the packet transmission in the network.

New node deployment is unavoidable because nodes in a sensor network may be lost or destroyed. In our proposed security protocol, we consider authentication of newly joining nodes and nodes that have left the network and re-joining. Without loss of generality, the proposed method will achieve two tasks:

1. Authentication of new nodes
2. Establishment of key: upon authentication, a shared key is created and provided to the deployed nodes to provide a secure communication.

The proposed protocol integrates the node authentication using the one-round ZKP [27] and the AES algorithm [28-29] for key establishment. The proposed model provides authentication for new nodes joining the network and the re-joining nodes to the network. The authentication of nodes is achieved by adapting one-round ZKP as proposed in [27]. Based on the protocol in our model, both base station and new node know generator g, b and prime number p. It is a challenge-and-response kind of protocol where new node has to prove in zero knowledge that it knows x such that

$$g^x = b(mod\,p)$$

In addition, BS generates a random y and computes

$$c = g^y(mod\;p)$$

The BS then, sends c as a challenge to new node. The new node responds the challenge by computing

$$r = c^x(mod\,p)$$

and sending r to BS. BS can verify the validity of new node's response by verifying that

$$r = b^y(mod\,p)$$

Upon authenticating the BS is responsible to issue the network key to the new node. The network key is generated by the base station using the AES algorithm as mentioned in [28]. This is the symmetric key that allows new node to join the network and for all nodes to encrypt and decrypt the messages transmitted between them. These keys ensure all the packets are kept secret so that eavesdroppers cannot intercept, modify and analyse, and discover valuable information transmitted along the network.

A. Assumptions

The following assumptions are made based on the proposed security protocol:

1. The base station acts as a controller, is secure, trustworthy and has powerful resources in terms of energy, memory and computation.
2. All the sensor nodes are similar in terms of energy, memory and computation capabilities. Each of them has unique ID.
3. The sensor nodes have enough memory to manage the keying overheads.
4. The base station and new node both know generator g, b and prime number p.

5. The keys are generated by the base station.
6. The base station is not compromised at anytime.

B. Security Protocol

1. New node sends "Add Me" message (M), unique ID to its neighbour nodes.
2. All neighbouring nodes call "SelectWinner" procedure [11] to determine one winner to communicate with the new node.
3. The selected winner then communicates with the base station (BS) and requests for the value of *c* [27].
4. BS generates a random number *y* and computes $c = g^y (mod\ p)$ and sends to the new node through the winner.
5. New node computes $r = c^x (mod\ p)$ and returns the value to the BS through the winner.
6. Base station verifies $r = b^x (mod\ p)$ from the received information and authenticates the new node.
7. Upon authenticating the new node, BS issues the network key to the new node. The network key is transmitted from BS to new node through the winner node.
8. Once new node receives the network key, the new node is able to join the network [29].
9. Then, new node calls the "simulate IN" procedure [11] to gather information from all neighbouring nodes such as node ID and status to determine its cluster.

Theorem 1: Let *CNet(G)* be a cluster based network of G, q be the number of neighbors of new node in G', and h is the number of hops from the new node to the base station. The time complexity of the DCWSN security protocol is $O(h + q)$.

Proof: The "SelectWinner" procedure in [11] requires $O(\log q)$ times. According to the protocol, in the authentication procedure, number of hops from the new node to base station is *h*, so the expected time for this operation is $O(h)$. Upon receiving the network key, the new node determines its cluster where the neighbors of new node in G' are numbered from 1 to q which require expected $O(q)$ rounds in [9]. Therefore, the security protocol for DCWSN consisting authentication and key distribution takes a total of

$$O(\log q) + O(h) + O(q) = O(h + q)$$

while $\log q$ is less significant than *q*.

□

V. Analysis

The efficiency and practicality of the proposed protocol is analysed in terms of security, computational complexity and communication overhead.

The integration of the one round ZKP and AES symmetric keys is believed to provide a comprehensive security for DCWSN. The one round ZKP approach is designed to eliminate the iterative feature of existing ZKPs. Although they are useful for many applications, iterative ZKPs have high computation and communication costs. The proposed protocol satisfies the requirements of the existing ZKPs, but run in one round, reducing the cost of ZKP substantially. In addition, this protocol provides both completeness and soundness in authenticating newly joining nodes where the probability of the new node in proving itself to the base station successfully is very high, similarly the probability of new node tricking the base station is very slim [30]. The ZKP is designed in such a manner that the base station is not able to obtain any information from the protocol. Here the verifier is not able to cheat the new node and pretend to the third party as well.

The computation time is linearly dependent to the amount of data being processed. The amount of computational energy consumed by a security protocol on a given microprocessor is determined by the number of rounds required by the processor to compute the protocol, which depends largely on the cryptographic algorithm code efficiency. The execution time and the battery consumed are proportional to the complexity of operations per round as proved by complexity equations derived. Furthermore, the number of data moves required is a challenge to affirm how much effect each type of low-level operation has in the performance of the schemes because data transfers are difficult to analyze with different register allocations that can be done by the compiler and state of the operation system.

In normal applications, 128 bits key is considered very secure hence going for higher key sizes would mean unnecessary wastage of resources for the added security that is actually not required. Thus it is necessary to define the adequate security as it varies from one application to another. AES has lower power consumption and is faster to compute, as well as being cryptographically more secure. For laptop devices with the capability of more than 100,000J batteries and larger, power usage from cryptographic algorithms is not a huge concern. But as for PDA devices and smaller ones, cryptographic algorithm selection should be taken seriously. This is due to the run time differences of 2:1 may result from improper choices [31].

The utmost importance of any battery-powered wireless device, especially sensor nodes is the optimising block cipher implementations towards low energy consumption and low computational overhead. Memory utilisation is also a critical concern since RAM and cache size is a precious resource in sensor nodes. Hence, code size optimisation and lightweight block cipher software implementations that meet operational requirements of WSNs are important as well.

VI. Conclusion and Future Work

Based on this paper, the security protocol integrates the one round ZKP authentication protocol and the AES algorithm. This protocol is a practical approach to distinguish authenticity of new nodes and the re-joining nodes to ensure they are authentic and malicious nodes are not implanted to disrupt the network. In addition, the protocol allows secured communication through the keying mechanism that encrypts and decrypts the packets to allow safe data transmission along the network. The main focus of this work is to provide authenticity for nodes joining the network and to facilitate a secured and efficient communication.

This security protocol can be used as a basis to develop a novel security mechanism for DCWSN. In future the security protocol to be developed for DCWSN may focus on providing other aspects sensor network such as data freshness. The adaption and flexibility of the security feature is anticipated to support DCWSN to be integrated with other network such as the cognitive radio networks (CRNs).

Acknowledgment

This work is fully supported by grant GUP Tier 2, 2011 with Reference No. Q.J130000.7143.00J93 and Malaysia-Japan International Institute of Technology (MJIIT) of Universiti Teknologi Malaysia (UTM).

References

[1] M. Y. Abdullah, G. W. Hua, “Cluster-based Security for Wireless Sensor Networks,” Conference on Communications and Mobile Computing, China, 2009.

[2] D. Westhoff, J. Girao, A. Sarma, "Security Solutions for Wireless Sensor Networks," Dependable IT and Network Technology, vol. 1, 2006

[3] L. Shen, X. Shi, "A dynamic Cluster based key management protocol in Wireless sensor network," International Journal of Intelligent Control and Systems, vol. 13, no. 2, June 2008, pp. 146-151

[4] S. Choi, V. Sarangan, J.Thomas, "Key Management in Wireless Sensor Networks with Internetwork," IEEE 2008.

[5] A. C. Ferreira, M. A. Vilaca, L. B. Oliveira, E. Habib, H. C. Wong, A. A. loureiro, "On the Security of Cluster-based Communication Protocols," 4th International Conference On Networking, Germany, vol. 1, pp. 449-458.

[6] R. Rautray, I. Sarangi, " A Survey On Authentication Protocols For Wireless Sensor Network”, International Journal of Engineering Science and Technology, Vol. 3, No. 5, 2011, pp. 4253-4256

[7] F. Yang, X. Zhou, "Distributed Node Authentication in Wireless Sensor Networks," 2nd International Conference on Future Computer and Communication (ICFCC), 2010, China, pp. 72-76

[8] C. T. Li, C. C. Lee, "A novel user authentication and privacy preserving scheme with smart cards for wireless communication," Mathematical and Computer Modelling , vol. 55, Iss. 1-2, pp. 35–44, 2012.

[9] A. S. K. Pathan, "Security in Wireless Sensor Networks: Issues and Challenges," The 8th International Conference Advanced Communication Technology, 2006. pp. 1048-1053

[10] D. Boyle, "Securing Wireless Sensor Networks: Security Architectures," Journal of Networks, vol. 3, no. 1, pp. 65-77, 2008.

[11] J. Uchida, A.K.M. M. Islam, Y. Katayama, W. Chen, and K. Wada, “Construction and maintenance of a novel cluster-based architecture for ad hoc sensor networks", Journal of Ad Hoc & Sensor Wireless Networks, Vol. 6 No. 1-2, 2008, pp. 1-31.

[12] W. Chen, A.K.M. M. Islam, M. Malkani, A. Shirkhodaie, K. Wada, and M. Z. Sabatto, “Novel broadcast/multicast protocols for dynamic sensor networks", To appear in the proceedings of the IEEE International Parallel & Distributed Processing Symposium 2007, USA

[13] A.K.M. M. Islam, K. Wada, J. Uchida, W. Chen, “A Better Dynamic Cluster-based Structure Wireless Sensor Network for Efficient Routing ", International Journal of Innovative Computing, Information and Control (IJICIC), Vol.8 No.10, October 2012, pp.1-11-0530.

[14] A.K.M. M. Islam, Y. Katayama, W. Chen, K. Wada, “A novel cluster-based architecture and a routing protocol for dynamic ad hoc radio networks", Journal of Electrical Engineering, The Institution of Engineers, Bangladesh, Vol. EE 33, No. I & II, December 2006

[15] B. Schoenmakers, "Part 1 Cryptographic Protocols," in Cryptography 2, MB Eindhoven, The Netherlands, Department of Mathematics and Computer Science, 2012, pp. 36-54.

[16] S. Keith, S. Lin, "Zero-Knowledge Proofs as Authentication Method in Wireless Sensor Networks," Cryptography and Network Security Final Project Report, 2011.

[17] A. M. Allam, I. I. Ibrahim, I. A. Ali, A. E. H. Elsawy, "Efficient Zero-Knowledge Identification Scheme with Secret Key Exchange," IEEE 46th Midwest Symposium on Circuits and Systems, 2003 , vol. 3, no. 04, pp. 227-230.

[18] "The Guillou-Quisquater Protocol (GQ)," 2011.

[19] Z. L. Gong, Guang, "A Survey on Security in Wireless Sensor Networks," University of Waterloo, Waterloo, Ontario, Canada, Ontario, 2011.

[20] Y. S. Jeong, "A Key Distribution method for Reducing Storage and Supporting High Level Security in the Large-scale WSN," International Journal of Digital Content Technology and its Applications, vol. 2, no. 1, pp. 61-66, 2008.

[21] M. K. Ghose, K. Sharma, "Security Model for Hierarchical Clustered Wireless Sensor," vol. 5, no. 1, 2011.

[22] S. S. S. J. S. Zhu, "Poster Abstract: LEAP – Efficient Security Mechanisms forLarge-Scale Distributed Sensor Networks," 2003.

[23] A. Hodjat and I. Verbauwhede. “Interfacing a high speed crypto accelerator to an embedded CPU”, In Proceedings of the 38th Asilomar Conference on Signals, Systems, and Computers, IEEE Press,vol. 1, pp. 488–492, 2004.

[24] B. Schneier, “Applied Cryptography:Protocols, Algorithms and Source Code in C”, John Wiley & Sons Inc. 2^{nd} Edition, 1996.

[25] A. Vitaletti, G. Palombizio: “Rijndael for Sensor Networks: Is Speed the Main Issue?” Electr. Notes Theor. Comput. Sci. 171(1): 71-81 (2007)

[26] MooSeop Kim, Juhan Kim, and Yongje Choi, "Low Power Circuit Architecture of AES Crypto Module for Wireless Sensor Network," in World Academy of Science, Engineering and Technology , 2005.

[27] S. Almuhammadi and C. Neuman “Security and Privacy Using One-Round Zero-Knowledge Proofs,” Proceedings of the Seventh IEEE International Conference on E-Commerce Technology (CEC’05), IEEE Press, vol.5, 2005

[28] M. Musa, E. Schaefer, and S. Wedig, “A simplified AES algorithm and its linear and differential Cryptanalyses, Cryptologia,” no.2, pp. 148-177, 2003

[29] Advanced Encryption Standard (AES), Vols. 197, NIST, 2001.

[30] Nadia M.G. Al Saidi, M.d. Said Muhamad Rushdan, “A New Idea in Zero Knowledge Protocols Based on Iterated Function Systems”, World Applied Sciences Journal, no.3, pp.364-371, 2011.

[31] N. R. Potlapally, S. Ravi, A. Raghunathin, and N. K. Jha, “Analyzing the Energy Consumption of Security Protocols”, In Proceedings. 2003 International Symposium on Low Power Electronics and Design, pp. 25-27, Aug. 2003.