International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 5 Issue 9, September-2016, Impact Factor: 1.544

Quantum Cryptograhy Integrated Effective Communication Approach for WPAN

Shally Nagpal

M. Tech. (Network Security), BPSMV Khanpur Kalan, Haryana

ABSTRACT

The communication becomes more critical when the network is having high speed mobility and restricted coverage. WPAN is one such network defined for indoor network and with smaller sensing limit. In this work, a quantum inspired encoded communication is provided to improve the communication reliability and security. The work model is defined for a randomly distributed and high mobility based WPAN network. At first phase of this model, the node level characterization is applied under coverage, stability and load parameters. Later on genetic model is applied to identify the most effective communication pair. Finally, the quantum key based SHA is applied to perform the data encoded. This encoded communication is performed over the network. The comparative results shows that the work model has reduced the communication loss over the network.

Keywords: WPAN, Genetics, Quantum, Encoded, Cryptography.

I. INTRODUCTION

Secure communication is the primary requirement of a network. Different detection based, preventive and the authentication methods are available to provide the secure and reliable communication in this network. To save the data from tampering and unauthorized access, one of the most familiar ways is to encode the data. Cryptography is one such method to provide the encoded communication. This encoded method not only prevents the information from intruder access but also saves the network from different active and passive attacks. The user level access control is provided by the cryptography method. It actually build a trust mechanism so that the secure communication is possible over the network. A standard cryptography model for encoded communication is shown here in figure 1.

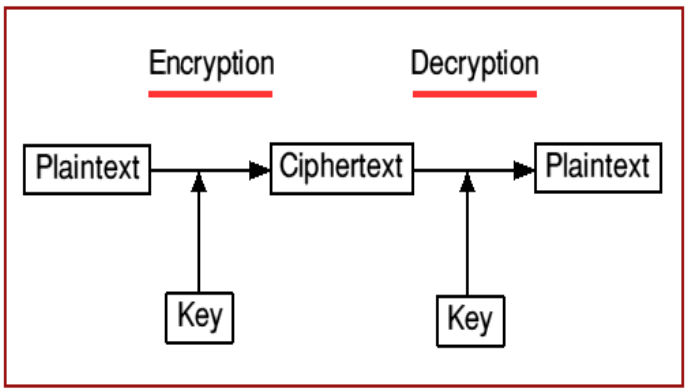

Figure 1 : Cryptography Method

Figure 1 here showing the cryptography process applied on sender and receiver side. On sender side, the plain data is taken as input and key specific encoding is done. This process is called encryption that transforms the input text to cipher text. After this, the encoded data is delivered to the receiver. On receiver side, the data decoding is done by using the same or the different key. This process of transforming the cipher text to plain text is called decryption. There is number cryptography method that varies according to the media type, key type or the algorithmic approach. The key used in these cryptography methods can be static or dynamic. The key generation and encoding method ensures the communication quality. In a dynamic network, the significance of dynamic key generation is higher so that the session based or the group adaptive or the region adaptive encoding will be done. In this work, a quantum cryptography model is provided to improve the communication security for sensor network.

A) Quantum Cryptography

Quantum Cryptography is the real time encoding method that captures the communication behavior or the physical characterization of the network and uses it to perform data encoding. It covers most of the uncertainty issues of network communication. The physical characterization used by the quantum cryptography method includes energy, momentum and the angular variation. The charge specific and session specific observations are also taken from the real time particles or atoms. These real time atoms are known as photons. The energy specific estimation is here defined to provide effective data encoding.

Different constraint and measures applied to capture the physical and the environment features so that the effective data encoding will be done. The behavior specific analysis is provided to extract the effective measurement based on which effective data encoding can be done. The medium specific analysis along with space time observation is defined to provide the effective data encoding. The quantum mechanics is here defined to provide the communication displacement and relatively applied some supervision method to provide effective encoding. The medium specific disruption can be defined to provide the data effective encoding. The positional observation is defined to provide the pattern specific encryption.

In this paper, quantum cryptography based communication model is provided for sensor network. The proposed work model has generated the genetic based key to identify the effective node pair. In this section, the requirement of security for a network is defined. The cryptography model and the characterization of quantum cryptography is provided in this paper. In section II, the work provided by the earlier researchers is discussed. In section III, the proposed work model is described. In section IV, thecomparative results obtained from the work are provided. In section V, the conclusion of the work is presented.

II. RELATED WORK

Different researchers already provided different encoding method to provide the secure communication in different methods. Different quantum cryptography based methods are also provided by the researchers. In this section, some of the work provided by earlier researchers is discussed. Author[1] has provided a three stage model to improve the quantum cryptography. The space model based communication is here integrated with quantum cryptography. The environment specific analysis along with key generation and distribution was provided by the author. The encoded communication control was provided by the author effectively. Author[2] has defined the use of quantum cryptography for communication process in the form of protocol.

The exploration of the methods and measure applied to generate the key parameters for quantum cryptography as well as to setup the relation uncertainty vector was provided by the author. Author[3] has defined the security management for quantum cryptography method. The physics law and methods are applied with network parameters to generate the keys and to provide the relatively adaptive network communication. Author[4] has defined a work on Zigbee protocol to provide the effective network security. The design specific estimation was provided with interconnection analysis so that the sub-network adaptive communication will be performed. Author[5] has provided work on different routing protocols specifically for sensor network. The Zigbee network standard was observed under AODV and DYMO protocols and relatively metrics based communication will be provided.

Author[6] has provided the work on coverset generation in sensor network and provided the tree adaptive communication. The work is defined as the event slot based communication provided to arrange the communication slots. Author[7] has defined a work on node uncertainty analysis to improve the target coverage in real time network. Author has defined the probabilistic estimation under various deficiencies. The grid specific coverage analysis is here provided to improve the node connectivity. The deployment error and placement errors are resolved by this algorithmic approach. Author[8] has performed the device specific improvement and establishment to the Zigbee network. The investigation was provided at node level so that the multiple communications is provided. Author[9] has worked on congestion adaptive Zigbee network generation.

The novel improved Zigbee protocol is defined against the delay, congestion and communication loss. The energy resource utilization was provided with protocol exploitation so that the collision adaptive communication will be obtained. Author[10] has provided an optimized solution to target coverage problem by arising the problem of minimum node selection. The work is defined to observe the node placement scheme and provided an area coverage method with improved k coverage with boundary specification to provide the region specific cover. The node division is done here under sleep node, listen node and active nodes.

Author[11] has provided a work on direction assignment and tunable node mapping to improve the target coverage with particular directional instance. The investigation is here provided to observe the target points so that the sensing area will be maximized. Author[12] has addressed one of the critical network issues to provide solution to the target

coverage problem. The network lifetime improvement with coverage ensurity is suggested in this work. The node process analysis with sensor activity observation is provided to control the energy dissipation. Author[13] has used the concept of weighted dynamic clustering environment with security integration. The analysis of this mobile sensor network is done with specification of five metrics. These metrics are able to identify the node criticality and able to sense the secure node for communication.

Author[14] has defined a trust metrics based observation on target coverage problem to provide the basic communication solution in effective way. A trust metric formulation is provided to ensure the coverage and provided an energy preserved way to provide the incorporated communication in the network. A target cover based preserving protocol is defined to observe the node stage so that the target region based node monitoring will be obtained. Author[15] has defined a work on event detection and optimization in real time environment to provide solution against sensing cover problem. The method includes the energy harvesting deployment of network under quality observation and duty cycle analysis.

III. RESEARCH METHODOLOGY

A personal area network is the critical restricted network with energy specification. The open network suffers from various internal and external attacks. To provide the safe communication, there is the requirement is to provide the effective encoded communication. In this work, a dynamic quantum key based cryptography model is provided for WPAN network. The presented work is here defined as an integrated work model in which the communication network is formed and later on applied the encoded communication over it using quantum cryptography. The work also integrated the genetic modeling to generate more adaptive communication pairs so that the reliable communication will be drawn over the network. The work stages relative to this provided work are shown in figure 2

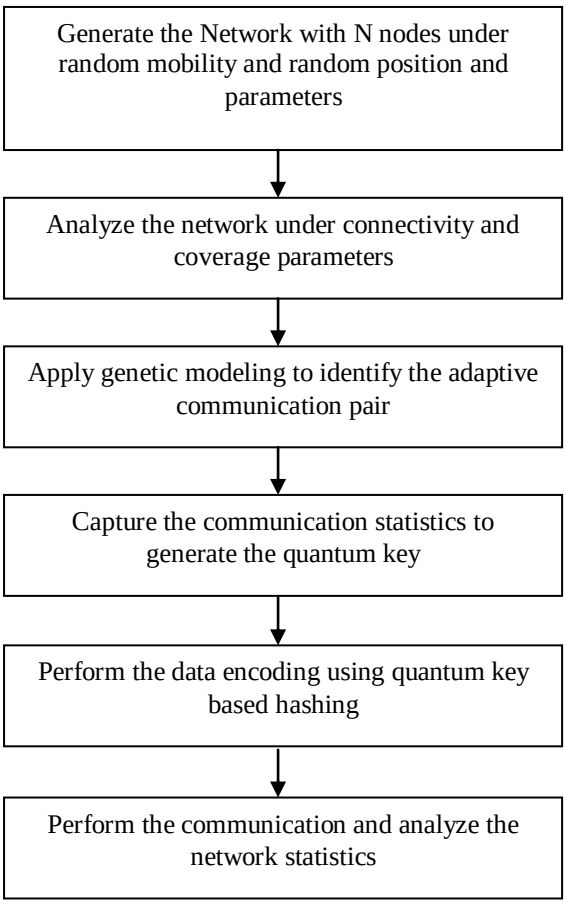

Figure 2: Proposed Work Model

Here figure 2 is showing the proposed work model. The figure is showing the communication model using quantum cryptography. At the earlier stage, the parameter specific network is composed using sensor network specification. Once the network is composed with specification of environmental and node specific constraints. The physical characterstics are generated for dynamic key for quantum cryptography modeling. Later on the genetic is applied to identify the effective node pair. Finally, the quantum encoded communication is performed over the network. The proposed work model is here defined in next section.

Genetics is the evolutionary process model that works on the biological process stages to generate the new population by applying some effective integrated process on initial and current population. The data driven generations are defined in controlled form with the specification of fitness function. The potential data analysis is applied to apply the fitness rule on this input data so that the effective and feasible data members will be generated. In this work, the genetic has accepted the node pairs as the possible connectivity and identified the most cost effective network connectivity. The work is to optimize the communication reliability. After specification of initial population, a series of iterative processes are applied to generate next level population and to provide the effective selection of effective key pairs. The next level generation and the specification of objective function are defined for final solution generation. In this work, the effective ranking map under load, coverage and failure parameters. The population is processed under the crossover and the mutation vectors for generating the next possible effective value. The process is repeated till the final optimized solution is not obtained.

IV. RESULTS

In this paper, a quantum integrated encoded communication model is provided for wireless personal network. The proposed work model is simulated in matlab environment. The network is here composed in a network region of 100x100 mtr. The fixed infrastructure devices are defined to control the communication. The mobile network with sensing capability is defined in the network. The quantum encoded communication is performed for 100 rounds and the comparative results are derived from the work. The existing work is here defined to perform the encoded communication using hash algorithm whereas the proposed work used the genetic optimized encoded communication. The comparative analysis in terms of packet loss is hsown here in figure 3.

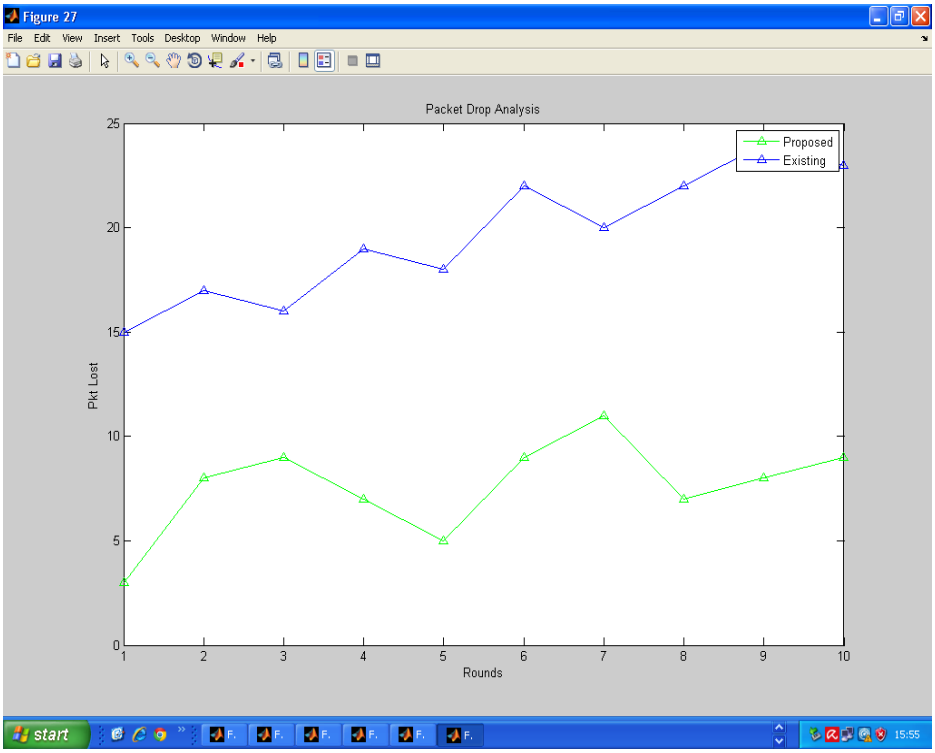

Figure 3 : Packet Loss Analysis (Existing Vs. Proposed)

Here figure is showing the comparative analysis in terms of packet loss. Here x axis showing the number of rounds and y axis showing the packet communication. The green line here represents the number of packet loss in case of proposed approach. The results shows that the method has reduced the packet loss over the network. The proposed work model has improved the integrity of work.

CONCLUSION

In this paper, a quantum improved encoded communication is provided for WPAN network. The network is defined with specification of infrastructure specification. The group adaptive encoded communication is performed. The genetic modeling is here defined to identify the effective node pair. The quantum based encoded communication is performed in this work. The simulation results shows that the proposed work model has reduced the packet loss over the network.

REFERENCES

[1]. S. Mandal et al., "Multi-photon implementation of three-stage quantum cryptography protocol," Information Networking (ICOIN), 2013 International Conference on, Bangkok, 2013, pp. 6-11.
[2]. A. Porzio, "Quantum cryptography: Approaching communication security from a quantum perspective," Photonics Technologies, 2014 Fotonica AEIT Italian Conference on, Naples, 2014, pp. 1-4.
[3]. M. Niemiec and A. R. Pach, "Management of security in quantum cryptography," in IEEE Communications Magazine, vol. 51, no. 8, pp. 36-41, August 2013.
[4]. Lei Zhou," A Simulation Platform for ZigBee-UMTS Hybrid Networks", IEEE COMMUNICATIONS LETTERS 1089-7798/13@ 2013 IEEE
[5]. Adam Dahlstrom," Performance Analysis of Routing Protocols in Zigbee Non- Beacon Enabled WSNs", Internet of Things: RFIDs, WSNs and beyond 978-1-4673-3133-3/13 ©2013 IEEE
[6]. Meng-Shiuan Pan," Convergecast in ZigBee Tree-Based Wireless Sensor Networks", 2013 IEEE Wireless Communications and Networking Conference (WCNC): NETWORKS 978-1-4673-5939-9/13 ©2013 IEEE
[7]. M. H. Shazly, E. S. Elmallah and J. Harms, "Location Uncertainty and Target Coverage in Wireless Sensor Networks Deployment," 2013 IEEE International Conference on Distributed Computing in Sensor Systems, Cambridge, MA, 2013, pp. 20-27.
[8]. Alexandru-Corneliu Olteanu," Enabling mobile devices for home automation using ZigBee", 2013 19th International Conference on Control Systems and Computer Science 978-0-7695-4980-4/13 © 2013 IEEE
[9]. R. Rostom, B. Bakhache, H. Salami and A. Awad, "Quantum cryptography and chaos for the transmission of security keys in 802.11 networks," Mediterranean Electrotechnical Conference (MELECON), 2014 17th IEEE, Beirut, 2014, pp. 350-356.
[10]. R. Khedikar and A. Kapur, "Energy effective target coverage WSNs," Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on, Ghaziabad, 2014, pp. 388-392.
[11]. Z. Lu and W. W. Li, "Approximation algorithms for maximum target coverage in directional sensor networks," Networking, Sensing and Control (ICNSC), 2014 IEEE 11th International Conference on, Miami, FL, 2014, pp. 155-160.
[12]. B. Diop, D. Diongue and O. Thiare, "A weight-based greedy algorithm for target coverage problem in wireless sensor networks," Computer, Communications, and Control Technology (I4CT), 2014 International Conference on, Langkawi, 2014, pp. 120-125.
[13]. A. Dahane, N. E. Berrached and A. Loukil, "Homogenous and secure weighted clustering algorithm for mobile wireless sensor networks," Control, Engineering & Information Technology (CEIT), 2015 3rd International Conference on, Tlemcen, 2015, pp. 1-6.
[14]. P. Chaturvedi and A. K. Daniel, "An Energy Efficient Node Scheduling Protocol for Target Coverage in Wireless Sensor Networks," Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference on, Gwalior, 2015, pp. 138-142.
[15]. X. Ren, W. Liang and W. Xu, "Quality-Aware Target Coverage in Energy Harvesting Sensor Networks," in IEEE Transactions on Emerging Topics in Computing, vol. 3, no. 1, pp. 8-21, March 2015.